University of Cincinnati

Date: 8/19/2015

I, Sergio D Molina Aristizabal , hereby submit this original work as part of the requirements for the degree of Doctor of Philosophy in Mathematical Sciences.

It is entitled:

Semi-Regular Sequences over F2

Student's name: **Sergio D Molina Aristizabal**

This work and its defense approved by:

Committee chair: Timothy Hodges, Ph.D.

Committee member: Donald French, Ph.D.

Committee member: Tara Smith, Ph.D.

19445

Semi-Regular Sequences over $\mathbb{F}_2$

A dissertion submitted to the

Division of Research and Advanced Studies
of the University of Cincinnati

in partial fulfillment of the
requirements for the degree of

Doctor of Philosophy

in the Department of Mathematical Sciences
of the College of Arts and Sciences

2015

by

Sergio Daladier Molina Aristizábal

B.S., Universidad Nacional de Colombia sede Medellin, 2005
M.S., Universidad Nacional de Colombia sede Medellin, 2009

Committee Chair: Timothy J. Hodges, Ph.D.

Abstract

The concept of semi-regular sequences was introduced in order to assess the complexity of Gröbner basis algorithms such as $\mathbf{F}_4$ for the solution of polynomial equations. Despite the experimental evidence that semi-regular sequences are common, it was unknown whether there existed semi-regular sequences for all n, except in extremely trivial situations. In the present work I prove some results on the existence and non-existence of semi-regular sequences. It was observed by J. Schlather and T. Hodges that if an element of degree d in $B^{(n)}$ is semi-regular, then we must have $n \leq 3d$. In this thesis, I establish precisely when the elementary symmetric polynomial of degree d is semi-regular. In particular, when $d = 2^t$ and $n = 3d$, the elementary symmetric polynomial of degree d is semi-regular establishing that the bound given by J. Schlather and T. Hodges is sharp for infinitely many n. For the general case of existence of semi-regular sequences the authors of [4] conjecture that the proportion $\pi(n, m, d_1, \ldots, d_m)$ of semi-regular sequences over $\mathbb{F}_2$ in the set $E(n, m, d_1, \ldots, d_m)$ of algebraic systems of m equations of degrees $d_1, \ldots, d_m$ in n variables tends to 1 as n tends to ∞. In this work, I show that for a fixed choice of $(m, d_1, \ldots, d_m)$, we have that $\lim_{n\to\infty} \pi(n, m, d_1, \ldots, d_m) = 0$ showing that the conjecture is false in this case.

A mi hija Valeria, mi esposa Mónica y mis padres Mireya e Iván

Acknowledgments

I would like to express my deepest gratitude to my advisor, Dr. Timothy J. Hodges, for his excellent guidance, breakthrough ideas, caring, patience, and encouragement throughout my graduate work. His guidance helped me in all the time of research and writing of this thesis.

I am so grateful to the State of Ohio scholarship scheme and the Department of Mathematical Sciences at University of Cincinnati for making it possible for me to study here. Furthermore, I would like to thank the Mazda Foundation of Colombia and COLFUTURO/Foundation for the future of Colombia for their financial support.

I thank the faculty and staff members of the Department of Mathematical Sciences at University of Cincinnati for supporting me through this process. In particular, I want to thank Dr. David Herron for the continuous encouragement.

I must also acknowledge and express my gratitude to my wife Mónica who was of essential support through the good and bad times.

Finally, I place on record, my sense of gratitude to all those, who directly or indirectly, supported me through this venture.

Table of Contents

CHAPTER 1

Introduction

One of the most classical mathematical problems is that of finding solutions to systems of polynomial equations of the form

$$p_1(X_1, \ldots, X_n) = \beta_1, \ldots, p_m(X_1, \ldots, X_n) = \beta_m.$$

This problem has been a central question in mathematics since earlier times, and arises in many fields such as algebraic geometry, statistics, game theory, and cryptography. In particular, systems of polynomial equations over a finite field play a fundamental role in multivariate public key cryptography (MPKC). A common and effective technique to solve such kind of systems of equations is to use a Gröbner basis algorithm. In 2004 Faugère et al. [3, 5, 4, 6] introduced the concept of semi-regular sequences to describe the most common and easily understandable systems. Although experimental evidence has shown that most sequences are semi-regular little progress has been made on the existence of such sequences. In this thesis we prove some of the first general results on the existence of semi-regular sequences.

MPKC systems are cryptographic systems based on multivariate polynomials over a finite field $\mathbb{F}_q$. In an MPKC system the public key is a set of polynomials $p_1(X_1, \ldots, X_n)$, $\ldots, p_m(X_1, \ldots, X_n) \in \mathbb{F}_q[X_1, \ldots, X_n]$, where $\mathbb{F}_q$ is a finite field. If Alice wants to send a message $(\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n$ to Bob, she computes $p_1(\alpha_1, \ldots, \alpha_n) = \beta_1, \ldots, p_m(\alpha_1, \ldots, \alpha_n) = \beta_m$,

and sends the encrypted message $(\beta_1, \ldots, \beta_m) \in \mathbb{F}_q^m$ to Bob. Bob's private key will be some secret information about the construction of the polynomials $p_1(X_1, \ldots, X_n), \ldots, p_m(X_1, \ldots, X_n)$ without which the system $p_1(X_1, \ldots, X_n) = \beta_1, \ldots, p_m(X_1, \ldots, X_n) = \beta_m$ should be computationally hard to solve. A number of MPKC systems, such as Matsumoto-Imai (MI) [30], Hidden Field Equations (HFE) [32], Sflash [33], Rainbow [17], have been proposed that involve quadratic functions over a finite field $\mathbb{F}_q$, especially over $\mathbb{F}_2$, the field of two elements. The HFE system works as follows. Let $\mathbb{F}$ be a field of order q and $\mathbb{K}$ an extension field of $\mathbb{F}$ of degree n. Define the function $P : \mathbb{K} \to \mathbb{K}$ by

$$P(X) = \sum_{q^i + q^j \leq D} a_{ij} X^{q^i + q^j} + \sum_{q^i \leq D} b_i X^{q^i} + c$$

and let $\tau, \sigma : \mathbb{F}^n \to \mathbb{F}^n$be two invertible affine maps. Consider the map $Q = \tau P \sigma^{-1} : \mathbb{F}^n \to \mathbb{F}^n$ as shown below

$$\begin{array}{ccc} \mathbb{K} & \xrightarrow{P} & \mathbb{K} \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \tau} \\ \mathbb{F}^n & \xrightarrow{Q} & \mathbb{F}^n \end{array}$$

Then, $Q = (p_1, \ldots, p_n)$ where $p_1, \ldots, p_n$ are mutivariate quadratic polynomials. The public key consists of the polynomials $p_1, \ldots, p_n$ and the private key consists of the maps τ, σ and P. If the parameter D is not too large then the equation $P(X) = Y'$ can be solved using the Berlekamp-Massey algorithm [2].

The security of the MPKC systems relies on the difficulty of solving a system of polynomial equations. Solving a system of quadratic equations over a finite field is an NP-hard problem [22]. However, the NP-hardness of this general problem does not necessarily guarantee the security of MPKC systems.

The main types of algorithms used to solve such systems of equations are the Gröbner basis algorithm introduced by Buchberger [7, 8] and its variants including the $\mathbf{F}_4$ and $\mathbf{F}_5$ introduced by Faugère [20, 19]; and the **XL** algorithms including **FXL** and **mutantXL**

[11, 9]. In particular, Faugère was able to break Patarin's first HFE challenge consisting of 80 quadratic equations in 80 variables with coefficients in GF(2), [21].

Let us briefly discuss the ideas of the Gröbner basis, $\mathbf{F}_4$ and **XL** algorithms.

Gröbner basis algorithm

Gröbner bases were introduced in 1965, together with an algorithm to compute them (Buchberger's algorithm), by Bruno Buchberger in his Ph.D. thesis [7]. The Gröbner bases concept has been proved to be a powerful tool for solving many important problems in algebra. Here we summarize some of the the main definitions and results of Gröbner bases theory without any proofs. In [12] the reader can find proofs and a more detailed introduction to Gröbner bases theory.

Let $R := k[X_1, \ldots, X_n]$ be the ring of polynomials in n variables over the field k.

Definition. A *monomial ordering*, $<$, is a total order on the set of monomials, M, in R that is compatible with the product and such that 1 is the smallest monomial.

Definition. Let M be the set of monomials in R. Let $f = \sum_{t \in M} a_t t \in R$ and a monomial order $<$ in R.

- The support of f is $supp(f) := \{t \in M \mid a_t \neq 0\}$.
- The leading monomial of f is $LM(f) := \max(supp(f))$.
- The leading coefficient of f is $LC(f) := a_t$, where $t = LM(f)$.
- The leading term of f is $LT(f) := LC(f)LM(f)$.

Theorem (Algorithm of Division)**.** Let $B = f_1, \ldots, f_m$ be a set of polynomials in R . Given $f \in R$ we have that f can be expressed as

$$f = a_1 f_1 + \cdots + a_m f_m + r$$

where $a_i \in R$ and if $r \neq 0$ then the leading monomials of the $f_i's$ do not divide that of r. One says that f *reduces* to r by B.

Definition. Given an ideal I in R, a set $G = \{g_1, \ldots, g_m\}$ of elements of I and a monomial order $<$, we say that G is a Gröbner basis for I with respect to a monomial order if

$$(LM(g_1), \ldots, LM(g_m)) = (LM(I))$$

Definition (S-polynomials)**.** Let $f, g \in R$ and $t = lcm(LM(f), LM(g))$. The S-polynomial of f and g is

$$S(f, g) = \frac{t}{LT(f)} f - \frac{t}{LT(g)} g$$

Theorem. Given an ideal I in R, a set $G = \{g_1, \ldots, g_m\}$ of elements of I is a Gröbner basis for I if and only if for all $i, j \in \{1, \ldots, m\}$ we have that $S(g_i, g_j)$ reduces to 0 by G.

Theorem (Hilbert Basis Theorem)**.** Every ideal I of R is finitely generated.

Now let us give a basic version of an algorithm to find a Gröbner basis for an ideal I of R:

Input A set of polynomials F that generates I.

Output A Gröbner basis G for I.

1. $G := F$
2. Choose a pair f, g of polynomials in G with $f \neq g$ and compute the S-polynomial, $S(f, g)$.
3. Reduce the S-polynomial $S(f, g)$ to r by G. If $r \neq 0$ then add it to G.
4. Repeat steps 2 and 3 until all possible pairs are considered, including those involving the new polynomials added in step 3.

5. Output G.

The algorithm terminates because it is consistently increasing the size of the monomial ideal generated by the leading terms of our set G, and the Hilbert basis theorem guarantees that any such ascending chain must eventually become constant.

$\mathbf{F}_4$ algorithm

The $\mathbf{F}_4$ algorithm was introduced by J.-C. Faugère in [20]. This algorithm uses the same mathematical principles as the Buchberger's algorithm in that it processes reduced S-polynomials pairs. However, the main difference from Buchberger's algorithm is that instead of selecting a single pair $f, g \in B$, B a set of generators of the ideal I, Faugère proposes to select a subset $G \subset B$ where G contains all pairs f, g in B such that the degree of $lcm(LT(f), LT(g))$ is minimal.

XL algorithm

The **XL** algorithm was introduced by Courtois, Klimov, Patarin and Shamir [11] and was proposed as an algorithm to solve overdetermined systems of polynomial equations. The idea of the XL algorithm, as applied to the solution of a system of m quadratic equations in n variables $f_1(X_1, \ldots, X_n) = 0, \ldots, f_m(X_1, \ldots, X_m) = 0$, is to fix a number $D > 2$ and to consider all polynomial equations of the following form $hf_j = 0$, for all arbitrary monomial h of degree $\leq D - 2$, and to solve the new system by Gauss elimination. Specifically, one applies an elimination process to the space of functions spanned by the $hf_j's$. When the dimension of the space spanned by the $hf_j's$ is close to the dimension of the space of all functions of degree $\leq D$ then this process yields univariate polynomials which can be solved using the Berlekamp-Massey algorithm.

It is important to understand the complexity of the Gröbner basis algorithms. Let $f(n)$ be the time taken for the algorithm to yield a solution on a system of $m(n)$ equations in

n-variables, where $m(n)$ is a linear function of n. The complexity is roughly the asymptotic behavior of $f(n)$. In [3, 5, 4, 6] it is shown that for certain families of "generic" sequences called *semi-regular* the complexity is exponential in the number of variables.

Let us summarize some of the results presented in [3, 5, 4, 6] for systems of polynomial equations over $\mathbb{F}_2$. Consider a system of polynomial equations $p_1(X_1, \ldots, X_n) = \beta_1, \ldots, p_m(X_1, \ldots, X_n) = \beta_m$, where $p_1(X_1, \ldots, X_n), \ldots, p_m(X_1, \ldots, X_n) \in \mathbb{F}_2[X_1, \ldots, X_n]$. Let λ_i be the homogeneous component of maximal degree of the polynomial p_i seen as an element of $B = \mathbb{F}_2[X_1, \ldots, X_n/(X_1^2, \ldots, X_n^2)$ and let $I = (\lambda_1, \ldots, \lambda_m)$ be the generated by the homogeneous polynomials $\lambda_1, \ldots, \lambda_m$ in B. Denote by B_d the set of homogeneous polynomials of degree d in the ring B. Similarly denote by I_d the set of homogeneous polynomials in I of degree d.

Definition. The degree of regularity of I is defined as

$$d_{reg}(I) = \min\{d \geq 0 \mid I \cap B_d = B_d\}$$

The degree of regularity of an ideal I plays a pivotal role in the analysis of the complexity of Gröbner basis computation, since this is the largest degree of any polynomial occurring in the Gröbner basis algorithm, [28]. Computing the degree of regularity of a homogeneous ideal I, in general requires a lot of work. However, when the sequence $\lambda_1, \ldots, \lambda_m$ that generates the ideal I is "semi-regular", the degree of regularity of is theoretically known. Roughly speaking, a semi-regular sequence is a sequence $\lambda_1, \ldots, \lambda_m$ of homogeneous elements in B for which no relations but the trivial ones ($\lambda_i\lambda_j = \lambda_j\lambda_i, \lambda_i^2 = 0$) occur; in other words, it is a sequence in which the polynomials are as independent of each other as possible. It is shown in [3, 5, 4, 6] that for a semi-regular sequence $\lambda_1, \ldots, \lambda_m \in B$ of homogeneous polynomials of degrees $d_1, \ldots, d_m$ the degree of regularity is given by the natural number $\operatorname{Ind} T_{n,m}(z)$ which is the degree at which the first non-positive coefficient of the series $T_{n,m}(z) = (1 +$

$z)^n / \prod_{i=1}^{m}(1+z^{d_i})$ occurs.

In order to understand the complexity of the Gröbner basis algorithm on semi-regular systems we need to understand the behavior of the $\operatorname{Ind} T_{n,m}(z)$ as $n \to \infty$. Using tools of asymptotic analysis [13, 10] it is shown that the asymptotic expansion of $T_{n,n}(z)$ is $0.090n + 1.00n^{1/3} - 1.58 + 1.41/n^{1/3} + O\left(1/n^{2/3}\right)$ [4, Proposition9]. This enables Bardet et al. to conclude that the complexity of the Gröbner basis algorithm for semi-regular systems of n quadratic equations in n variables, is exponential in n.

A similar approach was used by Yang, Chen and Courtois [36, 34, 35] to find complexity bounds for the **XL** algorithm.

In the works [3, 5, 4, 6] the authors conjectured that most sequences are semi-regular. However, little is known about the existence of such sequences beyond the experimental evidence. The present work represents our contribution to the understanding of semi-regular sequences over $\mathbb{F}_2$. In this work we begin by proving some results about characterization of semi-regular sequences over $\mathbb{F}_2$. We present more reliable proofs for the Hilbert characterization of semi-regularity and give a new homological characterization of semi-regularity over $\mathbb{F}_2$. Then, we prove our main results here some results on the existence and non-existence of semi-regular sequences. We first look at the most elementary case, that of semi-regular elements (or sequences of length one). In her thesis [3], Bardet asserts that the element $\sum_{1\leq i<j\leq n} x_i x_j$ is semi-regular for all n over $\mathbb{F}_2$. It was observed in [26, 15], that there are no quadratic semi-regular elements when $n > 6$, showing that the assertion made by Bardet is false. On the other hand it is trivial that elements of degree n and $n-1$ must be semi-regular. This raises the question: for which values of n, the number of variables, and d do there exist semi-regular elements of degree d in B? J. Schlather and T. Hodges proved that if an element of degree $d \geq 2$ in B is semi-regular, then we must have $n \leq 3d$. In this work,

I establish precisely when the symmetric element

$$\sigma_{d,n} = \sum_{1 \leq i_1 < \cdots < i_d \leq n} x_{i_1} \cdots x_{i_d}$$

is semi-regular. In particular I prove the following theorem

Theorem. Let $d \geq 2$, where $d = 2^m l$ with l an odd number, and m a non-negative integer. Then

(a) If $l > 1$, $\sigma_{d,n}$ is semi-regular if and only if $n = d, d+1, ..., d+2^{m+1}-1$.

(b) If $l = 1$, $\sigma_{d,n}$ is semi-regular if and only if $n = d, d+1, ..., d+2^{m+1}$.

Therefore, when $d = 2^t$, $\sigma_{d,n}$ is semi-regular for all $d \leq n \leq 3d$, thus establishing that the bound is sharp for infinitely many n.

For the general case of existence of semi-regular sequences the authors of [4] conjecture that the proportion $\pi(n, m, d_1, \ldots, d_m)$ of semi-regular sequences over $\mathbb{F}_2$ in the set $E(n, m, d_1, \ldots, d_m)$ of algebraic systems of m equations of degrees $d_1, \ldots, d_m$ in n variables tends to 1 as n tends to ∞. In this thesis I prove the following theorem

Theorem. Let $d_1, \ldots, d_m$ be a sequence of integers with $d_i \geq 2$ for some $1 \leq i \leq m$. Then there exists an N such that for all $n \geq N$, there cannot be a semi-regular sequence $\lambda_1, \ldots, \lambda_m$ of homogeneous polynomials of degrees $d_1, \ldots, d_m$.

This shows that for a fixed choice of $(m, d_1, \ldots, d_m)$, with $d_i \geq 2$ for some i, we have that

$$\lim_{n \to \infty} \pi(n, m, d_1, \ldots, d_m) = 0$$

In particular, this result tells us that underdetermined systems of polynomial equation (systems where there are fewer equations than unknowns) are not semi-regular when the number of unknowns is big enough compared to the number of equations. The results presented in this work represent the first significant progress about the existence of semi-regular sequences

over $\mathbb{F}_2$ since this concept was introduced in [3, 5, 4, 6] in 2004. Some of these results can be found in our paper [24].

The present work does not pretend to have an impact on the complexity analysis of the algorithms mentioned above but to extend our knowledge on semi-regular sequences. Although, these results give a better understanding of semi-regular sequences, it is still needed to prove the observed fact that "most" quadratic sequences of length n in n variables are semi-regular.

CHAPTER 2

Background

This chapter introduces some concepts, definitions and notation that will be used in the subsequent chapters. The presentation of this material is brief. We refer the reader to the original sources for more details.

2.1 Graded rings and Hilbert Series

This section introduces the concept of graded ring and Hilbert series. For more details basic sources are the books by D. Eisenbud [18, Sections 1.5, 1.9, 10.4, 12.1] and M. Atiyah and I. MacDonald [1, Chapters 10 and 11].

A ring R is called *graded* (or $\mathbb{Z}$-*graded*) if there exists a family of subgroups $\{R_n\}_{n\in\mathbb{Z}}$ of R such that

1. $R = \bigoplus_{n\in\mathbb{Z}} R_n$ as abelian groups
2. $R_n R_m \subset R_{n+m}$ for all n, m.

A graded ring R is called $\mathbb{N}$-*graded* if $R_n = 0$ for all $n < 0$. Elements of any factor R_n are called *homogeneous elements* of *degree* n. An ideal I of a graded ring is called a *graded* or *homogeneous ideal* if I is generated by homogeneous elements.

If I is a homogeneous ideal of graded ring R then R/I is also a graded ring and has

decomposition

$$R/I = \bigoplus_{n\in\mathbb{Z}} (R_n + I)/I$$

The classical example of a graded ring is the polynomial ring in n-variables over a field k, $R = k[X_1, \ldots, X_n]$. R is the direct sum of R_d where R_d is the set of homogeneous polynomials of degree d.

A module M over a graded ring R is called *graded* (or $\mathbb{Z}$-*graded*) if there exists a family of subgroups $\{M_n\}_{n\in\mathbb{Z}}$ of M such that

1. $M = \bigoplus_{n\in\mathbb{Z}} M_n$ as abelian groups
2. $R_n M_m \subset M_{n+m}$ for all n, m.

A morphism $f : N \to M$ between graded modules, called a *graded morphism*, is a morphism of modules such that $f(N_i) \subset M_i$ for all i.

Let R be a ring and let **ModR** be the category of finitely generated R-modules. An additive integer-valued function $\lambda : \mathbf{ModR} \to \mathbb{Z}$ is a function satisfying $\lambda(M) = \lambda(M') + \lambda(M'')$ for every short exact sequence

$$0 \to M' \to M \to M'' \to 0$$

in **ModR**. The most common examples of additive functions are:

1. $\lambda(M) = \dim_k M$, when R is a finitely generated algebra over a field k.
2. $\lambda(M) = \text{length}(M)$, when R is an Artinian ring.

An algebra A over a ring S is a *graded algebra* if it is graded as a ring. Suppose that A is an algebra over a field $k \subset A_0$ such that $\dim_k A_i < \infty$ for all i. The function $\text{HF}_A(i) = \dim_k A_i$ is called the *Hilbert function* of A. The *Hilbert series* of A is the formal power series given by

$$\text{HS}_A(z) = \sum_{i=0}^{\infty} (\dim_k A_i) z^i$$

If I is a graded ideal of A, then A/I has an induced graded ring structure. We define the Hilbert series of I to be the Hilbert series of the graded algebra A/I

$$\mathrm{HS}_I(z) = \sum_{i=0}^{\infty} \dim((A/I)_i) z^i$$

As an example, let $A = k[X_1, \ldots, X_n]$, be the ring of polynomials in n-variables. Thus,

$$\mathrm{HS}_A(z) = \sum_{i=0}^{\infty} \binom{n+i-1}{n-1} z^i$$

Using the fact that $\dim_k$ is an additive function in the category of finitely generated k-vector spaces we have the following theorem

Theorem 2.1.1. *If $A = k[X_1, \ldots, X_n]$, then*

$$HS_A(z) = \frac{1}{(1-z)^n}.$$

2.2 Associated graded rings

A *filtration* on a ring R is a set of subgroups of R,

$$R_0 \subset R_1 \subset R_2 \subset \cdots \subset \bigcup_i R_i = R$$

such that $R_i R_j \subset R_{i+j}$. If $\phi\colon R \to R'$ is surjective homomorphism of rings, and R has a filtration, then there is an induced filtration on R' given by the subgroups $R'_i = \phi(R_i)$.

Let R be a filtered ring with filtration $\{R_i\}_{i\in\mathbb{Z}}$. The *associated graded ring* is defined by

$$\mathrm{gr}(R) = \bigoplus_{i\in\mathbb{Z}} R_i/R_{i-1}$$

with multiplication given by the following rule: if $r+R_{i-1} \in R_i/R_{i-1}$ and $s+R_{j-1} \in R_j/R_{j-1}$, then

$$(r + R_{i-1})(s + R_{j-1}) = rs + R_{i+j-1}.$$

Let $R = F[X_1, \ldots, X_n]$ be the ring of polynomials over F, where F is a field of order q. Denote by $R_{(d)}$ the vector space over F of all polynomials of degree less than or equal to d, thus $\{R_{(d)}\}$ is a filtration on the ring R. Consider the algebras

$$A = F[X_1, \ldots, X_n]/(X_1^q - X_1, \ldots, X_n^q - X_n)$$

and

$$B = F[X_1, \ldots, X_n]/(X_1^q, \ldots, X_n^q)$$

Let $\phi\colon R \to A$ and $\gamma\colon R \to B$ be the usual projections. A has structure of filtered F-algebra with filtration given by $\{A_d := \phi(R_{(d)})\}$. B has structure of graded F-algebra with grading given by $\{B_d := \gamma(R_d)\}$, where R_d is the set of homogeneous polynomials of degree d.

The following theorem gives us the relation between the graded algebras B and $gr(A)$.

Theorem 2.2.1.

$$gr(A) \cong B$$

as graded F-algebras.

2.3 Complexes of Modules

This section gives some notions about complexes of modules and chains of complexes. For more details basic sources are the books by D. Eisenbud [18, Sections A3.5, A3.6, A3.7] and S. Lang [27, Chapter XX, sections 1, 2].

A *chain complex* $(C_\bullet, d_\bullet)$ is a sequence of R-modules $\ldots, C_2, C_1, C_0, C_{-1}, C_{-2}, \ldots$ and homomorphisms $d_i : C_i \to C_{i-1}$ such $d_{i-1} \circ d_i = 0$ for all i. A chain complex is usually written as

$$\cdots \to C_n \xrightarrow{d_n} C_{n-1} \xrightarrow{d_{n-1}} \cdots \to C_2 \xrightarrow{d_2} C_1 \xrightarrow{d_1} C_0 \xrightarrow{d_0} \cdots$$

Since $d_{i-1} \circ d_i = 0$ then $\operatorname{Im} d_i \subseteq \operatorname{Ker} d_{i-1}$. Thus, we can define the quotient

$$H_n(C_\bullet) = \operatorname{Ker} d_n / \operatorname{Im} d_{n+1}$$

called the n-th homology module of the complex $(C_\bullet, d_\bullet)$. The complex is *exact* in the n-th position if $H_n(C_\bullet) = 0$. The complex $(C_\bullet, d_\bullet)$ is *exact* if $\operatorname{Im} d_n = \operatorname{Ker} d_{n-1}$ for all n.

A *morphism of chain complexes* $f : (C_\bullet, d_\bullet) \to (C'_\bullet, d'_\bullet)$ is a sequence of homomorphisms $f_n : C_n \to C'_n$ for which the following diagram commutes

$$\begin{array}{ccc} C_n & \xrightarrow{f_n} & C'_n \\ \downarrow{\scriptstyle d_n} & & \downarrow{\scriptstyle d'_n} \\ C_{n-1} & \xrightarrow{f_{n-1}} & C'_{n-1} \end{array}$$

Notice that

$$f_n(\operatorname{Ker} d_n) \subseteq \operatorname{Ker} d'_n$$

and

$$f_n(\operatorname{Im} d_{n+1}) \subseteq \operatorname{Im} d'_{n+1}.$$

Together these allow us to define for each n a homomorphism

$$f_* : H_n(C_\bullet) \to H_n(C'_\bullet)$$

where $f_*(u + \operatorname{Im} d_{n+1}) = f_n(u) + \operatorname{Im} d'_{n+1}$.

Let $f : (A_\bullet, d^A_\bullet) \to (B_\bullet, d^B_\bullet)$ and $g : (B_\bullet, d^B_\bullet) \to (C_\bullet, d^C_\bullet)$ be two morphims of chain complexes. The sequence

$$0 \to A_\bullet \xrightarrow{f} B_\bullet \xrightarrow{g} C_\bullet \to 0$$

is called *exact* if for all n we have that the sequence

$$0 \to A_n \xrightarrow{f_n} B_n \xrightarrow{g_n} C_n \to 0$$

is exact.

Theorem 2.3.1. *Every exact sequence of chain complexes gives long exact sequence of homology*

$$\cdots \to H_{n+1}(C_\bullet) \xrightarrow{\sigma_{n+1}} H_n(A_\bullet) \xrightarrow{f} H_n(B_\bullet) \xrightarrow{g} H_n(C_\bullet) \xrightarrow{\sigma_n} H_{n-1}(A_\bullet) \to \cdots$$

where the homomorphisms σ_i are called the connecting homomorphisms.

Proof. See [27, Theorem 2.1, page 768]. □

CHAPTER 3

Semi-Regular Sequences

3.1 Semi-Regularity

Let us start reviewing the concept of regular sequence [18, Chapter 17]. Let R be a commutative ring and M an R-module. An element $r \in R$ is called a *non-zero-divisor on* M if every time that $rm = 0$ for some $m \in M$ implies that $m = 0$. A sequence $r_1, \ldots, r_n$ in R is called a *M-regular sequence* if for all $i = 1, \ldots, n$ we have that r_i is a non-zero-divisor on $M/(r_1, \ldots, r_{i-1})M$. An R-regular sequence is simply called a *regular sequence*.

Consider $S = k[X_1, \ldots, X_n]$ the ring of polynomials in n-variables over the field k. Let M be a $\mathbb{Z}$-graded S-module with finite length, that is, $M_n = 0$ for $n >> 0$, then clearly, there is no regular element on M. However, it could be the case that a polynomial is regular in M "up to some particular degree". It motivates the following definition given in [14].

Definition 3.1.1. Let M be a non-trivial finitely generated $\mathbb{Z}$-graded S-module. Let f be a homogeneous polynomial of degree d and D an integer. Then f is *regular up to degree D on M* if f is non-constant and for all $i \leq D-d$, the linear map $M_i \to M_{i+d}$ given by multiplication with f is injective. More generally, let $f_1, \ldots, f_r$ be a sequence of homogeneous polynomials and $D \in \mathbb{Z}$. Then the sequence is regular up to degree D on M if all the polynomials are non-constant and for each $q = 1, \ldots, r$, f_q is regular on $M/(f_1, \ldots, f_{q-1})M$ up to degree D.

Following the usual terminology, a sequence is simply called regular up to degree D if it fulfills the definition with $S = M$.

The notion of bounded regularity is closely related to the notion of *D-regularity* introduced in [3]: A sequence of homogeneous polynomials $f_1, \ldots, f_r$ in S is called D-regular if it is regular up to degree $D+1$ in the terms of [14]. Now, consider a sequence of homogeneous polynomials $f_1, \ldots, f_r$ in S and $I = (f_1, \ldots, f_r)$ the ideal generated by such sequence of polynomials. Note that S is a graded ring and I is a homogeneous ideal. Suppose that the quotient S/I is an Artinian ring. Then, the *degree of regularity* of I is defined as

$$d_{reg}(I) = \min\{d \geq 0 \mid I \cap S_d = S_d\}$$

Such sequence of homogeneous polynomials is called *semi-regular* if it is d_{reg}-regular. It is important to notice that this notion of semi-regularity presented in [3] and [6] has a different meaning from the one given in [31]. In [31] the notion of semi-regularity is as follows

Definition 3.1.2. Let I be a homogeneous ideal of S and let f be a homogeneous polynomial of degree d. Then f is semi-regular on S/I if for each $i \in \mathbb{Z}$ the linear map

$$(S/I)_i \xrightarrow{f} (S/I)_{i+d}$$

induced by multiplication by f is injective or surjective. Let now $f_1, \ldots, f_r$ be a sequence homogeneous polynomials. Then the sequence is semi-regular if for all $q = 1, ..., r$, we have that f_q is semi-regular on $S/(f_1, ..., f_{q-1})$.

Corollary 3.1.4 in this section states that permutations of semi-regular sequences under the notion presented in [3, 6] are also semi-regular. This does not hold for semi-regular sequences under notion [31]. An easy example for this is presented in [31]. The $x_2, y_2, xy \in k[x, y]$ is semi-regular but x_2, xy, y_2 is not.

The next theorem gives a characterization of semi-regular sequences in terms of Hilbert series (see Section 2.1). First, recall that the Hilbert function of a graded ring B is the function $HF_B(k) = \dim B_k$ and the Hilbert series is the series $HS_B(z) = \sum_{k=0}^{\infty}(\dim B_k)z^k$. The Hilbert function and series for a graded ideal I of B are defined by $HF_I = HF_{B/I}$ and $HS_I(z) = HS_{B/I}(z)$ respectively. For any series $a(z) = \sum_i a_i z^i \in \mathbb{R}[[z]]$, we define the index of $a(z)$, $\operatorname{Ind} a(z)$, to be the first t for which $a_t \leq 0$. If such a t does not exist define $\operatorname{Ind} a(z) = \infty$. For a series $\sum_i a_i z^i$, we denote by $[\sum_i a_i z^i]_t$ the truncated series $\sum_{i=0}^{t-1} a_i z^i$ and by $[\sum_i a_i z^i]$ the truncated series $[\sum_i a_i z^i]_{\operatorname{Ind}(a(z))}$.

Theorem 3.1.3. *Let $f_1, \ldots, f_m$ be a sequence of homogeneous polynomials of S with f_i being of degree d_i, such that $S/(f_1, \ldots, f_m)$ is Artinian. The sequence $f_1, \ldots, f_m$ is semi-regular if and only if*

$$HS_{S/(f_1,\ldots,f_m)}(z) = \left[\frac{\prod_{i=1}^{m}(1-z^{d_i})}{(1-z)^n}\right]$$

Proof. See [14], Proposition 1. □

Corollary 3.1.4. *Let $f_1, \ldots, f_m$ be a sequence of homogeneous polynomials of S with f_i being of degree d_i, such that $S/(f_1, \ldots, f_m)$ is Artinian. If the sequence $f_1, \ldots, f_m$ is semi-regular then so is $f_{\sigma(1)}, \ldots, f_{\sigma(m)}$ for any permutation σ.*

Proof. This result follows immediately from above theorem because the Hilbert series of $S/(f_1, \ldots, f_m)$ is independent of the order of the f_i. □

3.2 Semi-Regularity over $\mathbb{F}_2$

Set $B^{(n)} = \mathbb{F}_2[X_1, ..., X_n]/(X_1^2, ..., X_n^2)$ and define $B_k^{(n)}$ to be the subspace of homogeneous polynomials of degree exactly k. Then $B^{(n)} = \bigoplus_{k=0}^{n} B_k^{(n)}$ and $B_i^{(n)} B_j^{(n)} = B_{i+j}^{(n)}$, so this gives $B^{(n)}$ the structure of a strongly graded $\mathbb{F}_2$-algebra (see Section 2.1). Denote the image of X_i in $B^{(n)}$ by x_i.

The notion of semi-regularity over $\mathbb{F}_2$ for a sequence of homogeneous of the ring $B^{(n)}$ is slightly different from the one presented in Section 3.1. Given a homogeneous element $\lambda \in B^{(n)}$ of degree $d > 0$ we have that $\lambda^2 = 0$, thus the notion of semi-regularity is modified to have in account this behavior. This notion first appeared in [4].

Definition 3.2.1. For a graded ring $B = \bigoplus_{k=0}^{N} B_k$, we define the index of B to be t if $B_{t-1} \neq 0$ and $B_k = 0$ for all $k \geq t$. We denote this number by $\mathrm{Ind}(B)$. If $\lambda_1, \ldots, \lambda_m$ is a set of homogeneous elements and $I = (\lambda_1, \ldots, \lambda_m)$, then we define $\mathrm{Ind}(\lambda_1, \ldots, \lambda_m) = \mathrm{Ind}(B/I)$. If B is strongly graded (that is, $B_i B_j = B_{i+j}$ for all i and j), then

$$\mathrm{Ind}(B/I) = \min\{d \geq 0 \mid I \cap B_d = B_d\}$$

Definition 3.2.2. Let $\lambda_1, \ldots, \lambda_m$ be a sequence of homogeneous elements of $B^{(n)}$ of positive degree. The sequence $\lambda_1, \ldots, \lambda_m$ is *D-semi-regular over $\mathbb{F}_2$*, or simply *D-semi-regular*, if for all $i = 1, 2, \ldots, m$, if μ is homogeneous and

$$\mu\lambda_i \in (\lambda_1, \ldots, \lambda_{i-1}) \quad \text{and} \quad \deg(\mu) + \deg(\lambda_i) < D$$

then $\mu \in (\lambda_1, \ldots, \lambda_i)$. A sequence of homogeneous polynomials $\lambda_1, \ldots, \lambda_m$ is *semi-regular* if it is D-semi-regular for $D = \mathrm{Ind}(\lambda_1, \ldots, \lambda_m)$.

The concept of semi-regular sequence over $\mathbb{F}_2$ given in [6] is defined as follows

Definition 3.2.3. Let $\lambda_1, \ldots, \lambda_m$ be a sequence of homogeneous elements of $B^{(n)}$ of positive degree. Let $D = \mathrm{Ind}(\lambda_1, \ldots, \lambda_m)$. The sequence $\lambda_1, \ldots, \lambda_m$ is *semi-regular* if for all $i = 1, 2, \ldots, m$, if μ is homogeneous and

$$\mu\lambda_i \in (\lambda_1, \ldots, \lambda_{i-1}) \quad \text{and} \quad \deg(\mu\lambda_i) < D$$

then $\mu \in (\lambda_1, \ldots, \lambda_i)$.

However, we could have that $\mu\lambda_i = 0$, but in [6] it is not clear how is defined the degree of zero.

Now, we introduce the concept of D-semi-regularity over $\mathbb{F}_2$ in a more general context. Set $R = \mathbb{K}[X_1, ..., X_n]/(X_1^2, ..., X_n^2)$, with $\mathbb{K}$ a field of characteristic 2. Here and in the following, by a R-module we mean a $\mathbb{Z}$-graded R-module. Let M be a R-module. Given $d \in \mathbb{Z}$, we define $M(d)$ as the R-module M with grading $M(d)_i := M_{d+i}$. For $D \in \mathbb{Z}$ we set $M_{<D} := \bigoplus_{j<D} M_j$.

Definition 3.2.4. Let M be a non-trivial finitely generated R-module. Let $\lambda \in R$ be a homogeneous element of degree $d > 0$ and D an integer. Then λ is *D-semi-regular on M* if for all $i < D$ the map

$$(M/\lambda M)(-d)_i \xrightarrow{\lambda} M_i$$

given by multiplication by λ is injective. Notice that this map is well-defined since $\lambda^2 = 0$. More generally, let $\lambda_1, ..., \lambda_m$ be a sequence of homogeneous elements of positive degrees $d_1, ..., d_m$ and $D \in \mathbb{Z}$. Then the sequence is D-semi-regular on M if for all $i = 1, ..., m$, λ_i is D-semi-regular on $M/(\lambda_1, ..., \lambda_{i-1})M$. A sequence of homogeneous polynomials $\lambda_1, \ldots, \lambda_m \in R$ is *semi-regular* if it is D-semi-regular over R for $D = \mathrm{Ind}(\lambda_1, \ldots, \lambda_m)$.

In the case $M = R = B^{(n)}$ the definition of D-semi-regularity corresponds to the one given in Definition 3.2.2.

3.2.1 Characterization with Hilbert Series

Let M be a R-module as described above. Let $\mathrm{HS}_M(z) = \sum_{k=-\infty}^{\infty} (\dim M_k) z^k$ be the Hilbert series of M with associated Hilbert function $\mathrm{HF}_M(k) = \dim M_k$. For any $\mathbf{d} = (d_1, \ldots, d_m) \in \mathbb{N}^m$, define

$$T_{\mathbf{d},M}(z) = \frac{\mathrm{HS}_M(z)}{\prod_{i=1}^{m}(1 + z^{d_i})}$$

and let $t_{\mathbf{d},M}(j)$ be the coefficient of z^j in $T_{\mathbf{d},M}(z)$, so that $T_{\mathbf{d},M}(z) = \sum_{j=0}^{\infty} t_{\mathbf{d},M}(j) z^j$. Notice that in the case $M = R$ we have that $\mathrm{HS}_R(z) = (1+z)^n$. In this case we denote $T_{\mathbf{d},n}(z)$ by $T_{\mathbf{d},R}(z)$. It was asserted in [5] that a sequence $\lambda_1, \ldots, \lambda_m$ is semi-regular over $\mathbb{F}_2$ if and only if

$$\mathrm{HS}_{B^{(n)}/(\lambda_1,\ldots,\lambda_m)}(z) = [T_{\mathbf{d},n}(z)] = \left[\frac{(1+z)^n}{\prod_{i=1}^{m}(1+z^{d_i})}\right]$$

where $d_i = \deg \lambda_i$. As noted in [14], the proofs in that article are incomplete. We begin, therefore, by giving a complete proof. The proof of the main theorem, Theorem 3.2.6, is a joint work with Jacob Schlather and Dr. Timothy J. Hodges. This theorem was independently proved by J. Schlather and me. The proof presented here is an amalgamation of both proofs.

Let us start with some observations on the way truncation behaves with respect to multiplication.

Lemma 3.2.5. *Let $u(z), v(z), w(z) \in \mathbb{R}[[z]]$. Then*

1. $[u(z)v(z)]_D = [[u(z)]_D\,[v(z)]_D]_D = [u(z)\,[v(z)]_D]_D$
2. $[v(z)]_D = [w(z)]_D \implies [u(z)v(z)]_D = [u(z)w(z)]_D$

Proof. (1) First note that for any $a(z), c(z) \in \mathbb{R}[[z]]$,

$$[a(z) + c(z)z^D]_D = [a(z)]_D$$

Define $u'(z), v'(z)$ by $u(z) = [u(z)]_D + u'(z)z^D$ and $v(z) = [v(z)]_D + v'(z)z^D$. Then

$$\begin{aligned}
[u(z)v(z)]_D &= \left[([u(z)]_D + u'(z)z^D)([v(z)]_D + v'(z)z^D)\right]_D \\
&= \left[[u(z)]_D[v(z)]_D + z^D(u'(z)[v(z)]_D + v'(z)[u(z)]_D + u'(z)v'(z)z^D)\right]_D \\
&= [[u(z)]_D\,[v(z)]_D]_D
\end{aligned}$$

So

$$[u(z)\,[v(z)]_D]_D = [[u(z)]_D\,[v(z)]_D]_D = [u(z)v(z)]_D$$

(2) If $[v(z)]_D = [w(z)]_D$, then

$$[u(z)v(z)]_D = [u(z)[v(z)]_D]_D = [u(z)[w(z)]_D]_D = [u(z)w(z)]_D$$

□

Theorem 3.2.6. *Let $R = \mathbb{K}[X_1, ..., X_n]/(X_1^2, ..., X_n^2)$, with $\mathbb{K}$ a field of characteristic 2, let $\lambda_1, \ldots, \lambda_m$ be a sequence of homogeneous elements of R with λ_i being of degree d_i, and let M be a non-trivial finitely generated R-module. Set $I = (\lambda_1, \ldots, \lambda_m)$ and $\mathbf{d} = (d_1, \ldots, d_m)$.*

1. *If the sequence $\lambda_1, \ldots, \lambda_m$ is D-semi-regular on M then*

$$[HS_{M/IM}(z)]_D = [T_{\mathbf{d},M}(z)]_D$$

   and $HF_{M/IM}(D) \geq t_{\mathbf{d},M}(D)$.

2. *If the sequence $\lambda_1, \ldots, \lambda_m$ is D-semi-regular but not $(D+1)$-semi-regular, then $HF_{M/IM}(D) > t_{\mathbf{d},M}(D)$.*

3. *For $M = R$. The sequence $\lambda_1, \ldots, \lambda_m$ is semi-regular if and only if the Hilbert series of I is given by*

$$HS_I(z) = \left[\frac{(1+z)^n}{\prod_{i=1}^m (1+z^{d_i})}\right]$$

4. *If the sequence $\lambda_1, \ldots, \lambda_m$ is semi-regular, then so is $\lambda_{\sigma(1)}, \ldots, \lambda_{\sigma(m)}$ for any permutation σ.*

Proof. Set $\mathbf{d}_i = (d_1, \ldots, d_i)$ and denote $t_{\mathbf{d}_i,M}(d)$ by $t_i(d)$. Note that

$$(1 + z^{d_j}) \sum_{d=0}^{\infty} t_j(d) z^d = \sum_{d=0}^{\infty} t_{j-1}(d) z^d$$

so $t_{j-1}(d) = t_j(d) + t_j(d - d_j)$ for all j and d.

Set

$$s_i(d) = \mathrm{HF}_{M/(\lambda_1,\ldots,\lambda_i)M}(d) = \dim(M/(\lambda_1, \ldots, \lambda_i)M)_d$$

Let

$$K_i = \ker\left(M/(\lambda_1,\ldots,\lambda_i)M \xrightarrow{\lambda_i} M/(\lambda_1,\ldots,\lambda_{i-1})M\right),$$

let $K_{i,d}$ denote the subspace of degree d elements of K_i and let $k_i(d) = \dim K_{i,d}$. Note that $\lambda_1,\ldots,\lambda_m$ is D-semi-regular on M if and only if $k_i(d-d_i) = 0$ for all $d < D$ and all $i = 1,\ldots,m$.

We have an exact sequence

$$0 \to K_i \to M/(\lambda_1,\ldots,\lambda_i)M \xrightarrow{\lambda_i} M/(\lambda_1,\ldots,\lambda_{i-1})M \to M/(\lambda_1,\ldots,\lambda_i)M \to 0$$

which breaks up into exact sequences at degree d

$$0 \to K_{i,d-d_i} \to (M/(\lambda_1,\ldots,\lambda_i)M)_{d-d_i} \xrightarrow{\lambda_i} (M/(\lambda_1,\ldots,\lambda_{i-1})M)_d \to (M/(\lambda_1,\ldots,\lambda_i)M)_d \to 0$$

Taking the dimension of each term yields

$$k_i(d-d_i) - s_i(d-d_i) + s_{i-1}(d) - s_i(d) = 0$$

We now prove the assertions in part (1) by induction on m using the case $m = 0$ (the "empty sequence") as the base case. In this situation the assertions follow from the fact that $T_{\mathbf{d},M}(z) = HS_M(z)$. Now let $m > 0$. The hypothesis of D-semi-regularity implies that $s_{m-1}(d) = s_m(d) + s_m(d-d_m)$ for $d = 0,\ldots,D-1$. The induction hypothesis implies that $s_{m-1}(d) = t_{m-1}(d)$ for $d < D$. So

$$\begin{aligned}
[\mathrm{HS}_{M/(\lambda_1,\ldots,\lambda_{m-1})M}(z)]_D &= \sum_{d=0}^{D-1} s_{m-1}(d)z^d \\
&= \sum_{d=0}^{D-1} s_m(d)z^d + \sum_{d=0}^{D-1} s_m(d-d_m)z^d \\
&= (1+z^{d_m})\sum_{d=0}^{D-1} s_m(d)z^d \\
&= (1+z^{d_m})\left[\mathrm{HS}_{M/(\lambda_1,\ldots,\lambda_m)M}(z)\right]_D
\end{aligned}$$

Using Lemma 3.2.5 and induction on m yields

$$\begin{aligned}[\mathrm{HS}_{M/(\lambda_1,\ldots,\lambda_m)M}(z)]_D &= \left[\frac{1}{(1+z^{d_m})}[\mathrm{HS}_{M/(\lambda_1,\ldots,\lambda_{m-1})M}(z)]_D\right]_D \\ &= \left[\frac{1}{(1+z^{d_m})}\left[\frac{\mathrm{HS}_M(z)}{\prod_{j=1}^{m-1}(1+z^{d_j})}\right]_D\right]_D \\ &= \left[\frac{\mathrm{HS}_M(z)}{\prod_{j=1}^{m}(1+z^{d_j})}\right]_D\end{aligned}$$

which proves the first assertion. For the second part we assume, by induction, that $s_{m-1}(D) \geq t_{m-1}(D)$ and observe that by semi-regularity and the first part, $s_m(D-d_m) = t_m(D-d_m)$. Hence

$$\begin{aligned}s_m(D) &= s_{m-1}(D) - s_m(D-d_m) + k_m(D-d_m) \\ &\geq t_{m-1}(D) - t_m(D-d_m) = t_m(D)\end{aligned}$$

(2) Suppose that $\lambda_1,\ldots,\lambda_m$ is D-semi-regular but not $(D+1)$-semi-regular. Let u be the smallest integer such that $\lambda_1,\ldots,\lambda_u$ is not semi-regular. Then $k_u(D-d_u) > 0$, so

$$\begin{aligned}s_u(D) &= s_{u-1}(D) - s_u(D-d_u) + k_u(D-d_u) \\ &> t_{u-1}(D) - t_u(D-d_u) = t_u(D)\end{aligned}$$

Now suppose that $s_j(D) > t_j(D)$ for some $u \leq j < m$. Then

$$\begin{aligned}s_{j+1}(D) &= s_j(D) - s_{j+1}(D-d_{j+1}) + k_{j+1}(D-d_{j+1}) \\ &> t_j(D) - t_{j+1}(D-d_{j+1}) = t_{j+1}(D)\end{aligned}$$

So by induction, $s_m(D) > t_m(D)$.

(3) Suppose now that $M = R$ and the sequence $\lambda_1,\ldots,\lambda_m$ is semi-regular, and set $D = \mathrm{Ind}(I)$. Then $[\mathrm{HS}_I(z)]_D = [T_{\mathbf{d},n}(z)]_D$ by part (1) because the sequence is D-semi-regular. Because $D = \mathrm{Ind}(I)$, $\mathrm{HS}_I(z) = [\mathrm{HS}_I(z)]_D$. By (1), $t_m(d) = s_m(d) > 0$ for $d < D$

and $t_m(D) \leq s_m(D) = 0$, so $\mathrm{Ind}(T_{\mathbf{d},n}(z)) = D$. Thus

$$[T_{\mathbf{d},n}(z)] = [T_{\mathbf{d},n}(z)]_D = [\mathrm{HS}_I(z)]_D = \mathrm{HS}_I(z)$$

as required.

Conversely, suppose that $\mathrm{HS}_I(z) = [T_{\mathbf{d},n}(z)]$ and let $D = \mathrm{Ind}(T_{\mathbf{d},n}(z))$. Then by definition, D is the degree of regularity of the sequence $\lambda_1, \ldots, \lambda_m$. If the sequence $\lambda_1, \ldots, \lambda_m$ is not D-semi-regular, then there exists a $k < D$ such that it is k-semi-regular and not $(k+1)$-semi-regular. By part (2) we would then have that

$$s_m(k) > t_m(k)$$

That is, the k-th coefficient of $\mathrm{HS}_I(z)$ is strictly greater than the k-th coefficient of $T_{\mathbf{d},n}(z)$, contradicting the fact that $\mathrm{HS}_I(z) = [T_{\mathbf{d},n}(z)]$. Thus the sequence is D-semi-regular and hence semi-regular.

(4) follows immediately from (3) because the Hilbert series of R/I is independent of the order of the λ_i. □

It is natural to expect that information about the semi-regular sequences should give us information about arbitrary sequences. Since semi-regular sequences have as few relations as possible, we expect the ideal generated by a semi-regular sequence $(\nu_1, \ldots, \nu_m)$ to grow at least as quickly as the ideal generated by an arbitrary sequence $(\lambda_1, \ldots, \lambda_m)$. That is (if we use the notation $\sum a_i z^i \leq \sum b_i z^i \Leftrightarrow a_i \leq b_i$ for all i),

$$\mathrm{HS}_{(\lambda_1,\ldots,\lambda_m)}(z) \geq \mathrm{HS}_{(\nu_1,\ldots,\nu_m)}(z)$$

Thus it is tempting to expect for any sequence $\lambda_1, \ldots, \lambda_m$ that

$$\mathrm{HS}_{(\lambda_1,\ldots,\lambda_m)}(z) \geq [T_{\mathbf{d},n}(z)]\,.$$

The following example shows that this is not true.

Example 1. Consider the element

$$\lambda = x_1x_2 + x_3x_4 + x_5x_6 + x_7x_8 + x_9x_{10} + x_{11}x_{12}$$

in $B^{(12)}$ and let $I = (\lambda)$. Then, using [16, Theorem 2.1] we can calculate that

$$\mathrm{HS}_I(z) = 1 + 12z + 65z^2 + 208z^3 + 430z^4 + 584z^5 + 494z^6 + 208z^7 + 65z^8 + 12z^9 + z^{10}$$

while

$$\left[\frac{(1+z)^{12}}{1+z^2}\right] = 1 + 12z + 65z^2 + 208z^3 + 430z^4 + 584z^5 + 494z^6 + 208z^7 + z^8 + 12z^9 + 65z^{10}$$

Note also that in this case $\mathrm{Ind}((\lambda)) = \mathrm{Ind}(T_{(12),n}(z))$ but λ is not semi-regular. Thus the condition $\mathrm{Ind}(I) = \mathrm{Ind}(T_{\mathbf{d},n}(z))$ is not equivalent to semi-regularity.

It would be interesting to know whether $\mathrm{Ind}((\lambda_1, \ldots, \lambda_m)) \geq \mathrm{Ind}(T_{\mathbf{d},n}(z))$ for an arbitrary sequence $\lambda_1, \ldots, \lambda_m$. All known evidence points to this result being true. However, the failure of the inequality $\mathrm{HS}_I(z) \geq [T_{\mathbf{d},n}(z)]$ rules out the obvious way of proving it.

3.2.2 Homological Characterization

In this section we give a homological characterization of D-semi-regularity over $\mathbb{F}_2$. First, we construct a complex using the idea of the tensor product of two chain complexes, this is one of the methods to construct the Koszul complex [18, Chapter 17]. This construction allows us to give a homological characterization of the D-semi-regularity over $\mathbb{F}_2$.

Let us review the tensor product of two chain complexes

Definition 3.2.7. Let S be a commutative ring. Let

$$X_\bullet : \cdots \longrightarrow X_n \xrightarrow{\partial_n^X} X_{n-1} \longrightarrow \cdots$$

and

$$Y_\bullet : \cdots \longrightarrow Y_n \xrightarrow{\partial_n^Y} Y_{n-1} \longrightarrow \cdots$$

be two complexes of S-modules. Then we form the complex $X_\bullet \otimes_S Y_\bullet$ by

$$(X_\bullet \otimes_S Y_\bullet)_i = \bigoplus_{p+q=i} (X_p \otimes_S Y_q)$$

and the boundary map $\partial_i^{X\otimes Y} : (X_\bullet \otimes_S Y_\bullet)_i \longrightarrow (X_\bullet \otimes_S Y_\bullet)_{i-1}$ given by

$$\partial_i^{X\otimes Y}(x_p \otimes y_q) = (\partial_p^X(x_p)) \otimes y_q + (-1)^p x_p \otimes (\partial_q^Y(y_q)).$$

Let $\lambda \in R = \mathbb{K}[X_1, ..., X_n]/(X_1^2, ..., X_n^2)$, with $\mathbb{K}$ a field of characteristic 2, be a homogeneous element of positive degree $d > 0$. We denote $\mathcal{K}(\lambda)$ by the complex

$$\mathcal{K}(\lambda) : 0 \longrightarrow R/(\lambda) \xrightarrow{\lambda} R \longrightarrow 0.$$

Proposition 3.2.8. *Let $\lambda \in R$ be a homogeneous element of positive degree. Let $\mathcal{C} : \cdots \longrightarrow C_n \xrightarrow{\partial_n^C} C_{n-1} \longrightarrow \cdots$ be a complex of R-modules. We have an exact sequence of complexes*

$$0 \to \mathcal{C} \to \mathcal{C} \otimes \mathcal{K}(\lambda) \to \mathcal{C}' \to 0$$

where $\mathcal{C}'$ is the complex such that $(\mathcal{C}')_n = C_{n-1}/\lambda C_{n-1}$ and the differential is is given by

$$\partial_n^{\mathcal{C}'}(\overline{a}) = \overline{\partial_{n-1}^{\mathcal{C}}(a)}$$

The homology exact sequence has the form

$$\cdots \longrightarrow H_n(\mathcal{C}) \longrightarrow H_n(\mathcal{C} \otimes \mathcal{K}(\lambda)) \longrightarrow H_n(\mathcal{C}') \xrightarrow{(-1)^{n-1}\lambda} H_{n-1}(\mathcal{C})$$
$$\longrightarrow H_{n-1}(\mathcal{C} \otimes \mathcal{K}(\lambda)) \longrightarrow H_{n-1}(\mathcal{C}') \longrightarrow \cdots$$

(the connecting map is given by multiplication by $\pm\lambda$. Note that $\pm\lambda = \lambda$, since $\mathbb{K}$ is a field of characteristic 2).

Proof. Notice that $(\mathcal{C} \otimes \mathcal{K}(\lambda))_n = (C_n \otimes R) \oplus (C_{n-1} \otimes R/(\lambda))$, which under the canonical identifications is $C_n \oplus (C_{n-1}/\lambda C_{n-1})$. Thus the complex $\mathcal{C} \otimes \mathcal{K}(\lambda)$ is given by

$$\cdots \longrightarrow C_n \oplus (C_{n-1}/\lambda C_{n-1}) \longrightarrow C_{n-1} \oplus (C_{n-2}/\lambda C_{n-2}) \longrightarrow \cdots$$

$$\cdots \longrightarrow C_1 \oplus (C_0/\lambda C_0) \longrightarrow C_0 \longrightarrow 0$$

Let us see that the boundary map is given by

$$\begin{aligned}\partial_n^{\mathcal{C}\otimes\mathcal{K}(\lambda)}(\varepsilon,\overline{\eta}) &= (\partial_n^{\mathcal{C}}(\varepsilon)+(-1)^{n-1}\lambda\eta, \overline{\partial_{n-1}^{\mathcal{C}}(\eta)}) \\ &= \partial_n^{\mathcal{C}}(\varepsilon)+\lambda\eta, \overline{\partial_{n-1}^{\mathcal{C}}(\eta)}.\end{aligned}$$

Consider $(\varepsilon\otimes r')\in C_n\otimes R$. Then $\partial_n^{\mathcal{C}\otimes\mathcal{K}(\lambda)}(\varepsilon\otimes r')=\partial_n^{\mathcal{C}}(\varepsilon)\otimes r'\in C_{n-1}\otimes R$, since $\mathcal{K}(\lambda)$ has no module in degree -1. Now, consider $(\eta\otimes\overline{r})\in C_{n-1}\otimes R/(\lambda)$, then $\partial_{n-1}^{\mathcal{C}\otimes\mathcal{K}(\lambda)}(\eta,\overline{r})=\partial_{n-1}^{\mathcal{C}}(\eta)\otimes\overline{r}+(-1)^{n-1}\eta\otimes\lambda r$. Notice that $\partial_{n-1}^{\mathcal{C}}(\eta)\otimes\overline{r}\in C_{n-2}\otimes R/(\lambda)$ and $(-1)^{n-1}\eta\otimes\lambda r\in C_{n-1}\otimes R$. Thus, under the canonical identifications $C_i\otimes R$ with C_i and $C_j\otimes R/(\lambda)$ with $C_j/\lambda C_j$ it follows that the boundary map in $\mathcal{C}\otimes\mathcal{K}(x)$ takes the required form.

The exactness follows easily by considering the following diagram

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & C_n & \to & C_n\oplus(C_{n-1}/\lambda C_{n-1}) & \to & (C_{n-1}/\lambda C_{n-1}) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & C_{n-1} & \to & C_{n-1}\oplus(C_{n-2}/\lambda C_{n-2}) & \to & (C_{n-2}/\lambda C_{n-2}) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & C_1 & \to & C_1\oplus(C_0/\lambda C_0) & \to & (C_0/\lambda C_0) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & C_0 & \to & C_0 & \to & 0 & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

By Theorem 2.3.1 we always we have a long homology exact sequence. Let us see that the connecting homomorphism in the long exact sequence on homology is multiplication

by λ. Let $\overline{\eta} \in C_{n-1}/\lambda C_{n-1}$ such that $\overline{\eta} \in \mathrm{Ker}(\partial_n^{\mathcal{C}'}) = \mathrm{Ker}(\ \overline{\partial_{n-1}^{\mathcal{C}}})$. Thus, $\partial_n^{\mathcal{C}\otimes\mathcal{K}(\lambda)}(0,\ \overline{\eta}) = (0 + \lambda\eta, 0) \in C_{n-1} \oplus (C_{n-2}/\lambda C_{n-2})$ and a preimage of this element under the map

$$C_{n-1} \to C_{n-1} \oplus (C_{n-2}/\lambda C_{n-2})$$

is $\lambda\eta$, which is what we wanted to show. □

Let $\mathcal{C} : \cdots \longrightarrow C_n \xrightarrow{\partial_n^C} C_{n-1} \longrightarrow \cdots$ be a complex of $\mathbb{Z}$-graded R-modules. For $d \in \mathbb{Z}$, we denote by $\mathcal{C}(d)$ the complex obtained from $\mathcal{C}$ by degree shift; i.e., $(\mathcal{C}(d))_i = C_i(d)$.

Given a sequence $\lambda_1, ..., \lambda_m$ of homogeneous elements of positive degrees $d_1, ..., d_m$, we define $\mathcal{K}(\lambda_1, ..., \lambda_m)$ as the tensor product $\mathcal{K}(\lambda_1) \otimes \cdots \otimes \mathcal{K}(\lambda_m)$. As an example,

$$\begin{aligned}\mathcal{K}(\lambda_1, \lambda_2) : 0 \ &\to \left(\tfrac{R}{(\lambda_1)}(-d_1 - d_2)\right) \otimes \left(\tfrac{R}{(\lambda_2)}(-d_1 - d_2)\right) \\ &\to \left(\tfrac{R}{(\lambda_1)}(-d_1)\right) \oplus \left(\tfrac{R}{(\lambda_2)}(-d_2)\right) \to R \to 0\end{aligned}$$

where given $(\overline{x}, \overline{y}) \in (R/(\lambda_1)(-d_1)) \oplus (R/(\lambda_2)(-d_2))$ then $\partial(\overline{x}, \overline{y}) = \lambda_1 x + \lambda_2 y$. And, given $\overline{x} \otimes \overline{y} \in (R/(\lambda_1)(-d_1 - d_2)) \otimes (R/(\lambda_2)(-d_1 - d_2))$ then $\partial(\overline{x} \otimes \overline{y}) = (\lambda_2\overline{xy}, \lambda_1\overline{xy})$. Using the natural identification $M \otimes_R (R/I) \simeq M/IM$, we see that the complex $\mathcal{K}(\lambda_1, \lambda_2)$ is given by

$$0 \ \to \left(\tfrac{R}{(\lambda_1,\lambda_2)}(-d_1 - d_2)\right) \to \left(\tfrac{R}{(\lambda_1)}(-d_1)\right) \oplus \left(\tfrac{R}{(\lambda_2)}(-d_2)\right) \to R \to 0$$

Also, when we consider $e_{12} = 1$ in $R/(\lambda_1, \lambda_2)$, $e_1 = 1$ in $R/(\lambda_1)$, and $e_2 = 1$ in $R/(\lambda_2)$, then $\partial(e_{12}) = \lambda_2 e_1 + \lambda_1 e_2$, $\partial(e_1) = \lambda_1$, $\partial(e_2) = \lambda_2$. By induction we can check that

$$\begin{aligned}\mathcal{K}(\lambda_1, ..., \lambda_m) : 0 \to \cdots \to \bigoplus_{1\le i_1<\cdots<i_r\le m} \left(\tfrac{R}{(\lambda_{i_1},...,\lambda_{i_r})}(-d_{i_1} - \cdots - d_{i_r})\right) \to \\ \cdots \to \bigoplus_{1\le i<j\le m} \left(\tfrac{R}{(\lambda_i,\lambda_j)}(-d_i - d_j)\right) \to \bigoplus_{1\le i\le m} \left(\tfrac{R}{(\lambda_i)}(-d_i)\right) \to R \to 0.\end{aligned}$$

If $e_{i_1,...,i_r}$ is the unity of $R/(\lambda_{i_1}, ..., \lambda_{i_r})$ we have that

$$\partial(e_{i_1,...,i_r}) = \sum_{l=1}^{r} \lambda_{i_l} e_{i_1,...,\widehat{i_l},...,i_r}$$

Notice that $H_0(\mathcal{K}(\lambda_1,...,\lambda_m)) = R/(\lambda_1,...,\lambda_m)$. For the complex $M \otimes \mathcal{K}(\lambda_1,...,\lambda_m)$ we have

$$0 \to \cdots \to \bigoplus_{1\leq i_1<\cdots<i_r\leq m} \left(\tfrac{M}{(\lambda_{i_1},...,\lambda_{i_r})M}(-d_{i_1}-\cdots-d_{i_r})\right) \to \cdots$$
$$\to \bigoplus_{1\leq i<j\leq m} \left(\tfrac{M}{(\lambda_i,\lambda_j)M}(-d_i-d_j)\right) \to \bigoplus_{1\leq i\leq m} \left(\tfrac{M}{(\lambda_i)M}(-d_i)\right) \to M \to 0$$

where for $[m]_{i_1,...,i_r} \in (M/(\lambda_{i_1},...,\lambda_{i_r})M)(-d_{i_1}-\cdots-d_{i_r})$ ($[m]_{i_1,...,i_r}$ meaning the class of $m \in M(-d_{i_1}-\cdots-d_{i_r})$ module $(\lambda_{i_1},...,\lambda_{i_r})M$) we have that

$$\partial([m]_{i_1,...,i_r}) = \sum_{l=1}^{r} [\lambda_{i_l} m]_{i_1,...,\widehat{i_l},...,i_r}$$

with analogous meaning for $[\lambda_{i_l} m]_{i_1,...,\widehat{i_l},...,i_r}$.

Lemma 3.2.9. *Let M be a finitely generated non-trivial R-module. Let $\lambda_1,...,\lambda_k$ be a sequence of homogeneous elements of positive degrees $d_1,...,d_k$, let D be a natural number. If $H_1(M\otimes\mathcal{K}(\lambda_1,...,\lambda_k))_{<D} = 0$ then for all $1 \leq i < k$ we have that $H_1(M\otimes\mathcal{K}(\lambda_1,...,\lambda_i))_{<D} = 0$.*

Proof. Notice that we only need to prove the result for $i = k-1$. Consider the complexes

$$\mathcal{C} = M \otimes \mathcal{K}(\lambda_1,...,\lambda_{k-1}) :$$
$$0 \to \cdots \to \bigoplus_{1\leq i<j\leq k-1} \left(\tfrac{M}{(\lambda_i,\lambda_j)M}(-d_i-d_j)\right) \xrightarrow{\delta_2} \bigoplus_{1\leq i\leq k-1} \left(\tfrac{M}{(\lambda_i)M}(-d_i)\right) \xrightarrow{\delta_1} M \to 0$$

$$\mathcal{C} \otimes \mathcal{K}(\lambda_k) = M \otimes \mathcal{K}(\lambda_1,...,\lambda_k) :$$
$$0 \to \cdots \to \bigoplus_{1\leq i<j\leq k} \left(\tfrac{M}{(\lambda_i,\lambda_j)M}(-d_i-d_j)\right) \xrightarrow{\sigma_2} \bigoplus_{1\leq i\leq k} \left(\tfrac{M}{(\lambda_i)M}(-d_i)\right) \xrightarrow{\sigma_1} M \to 0$$

$$\mathcal{C}' :$$
$$0 \to \cdots \xrightarrow{\overline{\delta_2}} \frac{\left(\bigoplus_{1\leq i\leq k-1}\left(\tfrac{M}{(\lambda_i)M}(-d_i)\right)\right)}{\lambda_k\left(\bigoplus_{1\leq i\leq k-1}\left(\tfrac{M}{(\lambda_i)M}(-d_i)\right)\right)} \xrightarrow{\overline{\delta_1}} \tfrac{M}{\lambda_k M} \to 0 \to 0$$

Notice that in general

$$\frac{\bigoplus_{1\leq i_1<\cdots<i_r\leq k-1} \left(\tfrac{M}{(\lambda_{i_1},...,\lambda_{i_r})M}(-d_{i_1}-\cdots-d_{i_r})\right)}{\lambda_k\left(\bigoplus_{1\leq i_1<\cdots<i_r\leq k-1} \left(\tfrac{M}{(\lambda_{i_1},...,\lambda_{i_r})M}(-d_{i_1}-\cdots-d_{i_r})\right)\right)}$$

is isomorphic to

$$\bigoplus_{1\leq i_1<\cdots<i_r\leq k-1}\left(\frac{M}{(\lambda_{i_1},...,\lambda_{i_r},\lambda_k)M}(-d_{i_1}-\cdots-d_{i_r})\right)$$

Thus, we have

$$\begin{aligned}\mathcal{C}':0\to\cdots\to \quad & \bigoplus_{1\leq i<j\leq k-1}\left(\tfrac{M}{(\lambda_i,\lambda_j,\lambda_k)M}(-d_i-d_j)\right)\xrightarrow{\overline{\delta_2}}\\ & \bigoplus_{1\leq i\leq k-1}\left(\tfrac{M}{(\lambda_i,\lambda_k)M}(-d_i)\right)\xrightarrow{\overline{\delta_1}}M/\lambda_kM\to 0\to 0\end{aligned}$$

where $\overline{\delta_2}([m]_{ijk})=[\lambda_jm]_{ik}+[\lambda_im]_{jk}$, and $\overline{\delta_1}([m]_{ik})=[\lambda_im]_k$. Let us show that $H_2(\mathcal{C}')_{<D}=0$. Let $l<D$. At level l we have the complex

$$\begin{aligned}(M\otimes\mathcal{K}(\lambda_1,...,\lambda_k))_l:0\to\cdots\to \quad & \left[\bigoplus_{1\leq i<j\leq k}\left(\tfrac{M}{(\lambda_i,\lambda_j)M}(-d_i-d_j)\right)\right]_l\xrightarrow{\sigma_2}\\ & \left[\bigoplus_{1\leq i\leq k}\left(\tfrac{M}{(\lambda_i)M}(-d_i)\right)\right]_l\xrightarrow{\sigma_1}M_l\to 0\end{aligned}$$

Since $H_1(M\otimes\mathcal{K}(\lambda_1,...,\lambda_k))_l=0$, then at this level $\mathrm{Ker}(\sigma_1)=\mathrm{Im}(\sigma_2)$. We want to show that $H_2(\mathcal{C}')_l=0$. In other words, we want to show that at level l we have that $\mathrm{Ker}(\overline{\delta_1})=\mathrm{Im}(\overline{\delta_2})$. Consider

$$\underset{1\leq i\leq k-1}{\oplus}[m_i]_{ik}\in\left[\bigoplus_{1\leq i\leq k-1}\left(\frac{M}{(\lambda_i,\lambda_k)M}(-d_i)\right)\right]_l$$

such that

$$\underset{1\leq i\leq k-1}{\oplus}[m_i]_{ik}\in\mathrm{Ker}(\overline{\delta_1})$$

Notice that $m_i\in M(-d_i)_l$. Since

$$\underset{1\leq i\leq k-1}{\oplus}[m_i]_{ik}\in\mathrm{Ker}(\overline{\delta_1})$$

then

$$[\lambda_1m_1]_k+\cdots+[\lambda_{k-1}m_{k-1}]_k=0\in M/\lambda_kM.$$

Therefore, there exits $m\in M$ such that

$$\lambda_1m_1+\cdots+\lambda_{k-1}m_{k-1}+\lambda_km=0\in M. \tag{3.1}$$

Consider the element

$$([m_1]_1, \ldots, [m_{k-1}]_{k-1}, [m]_k) \in \left[\bigoplus_{1\leq i\leq k}\left(\frac{M}{(\lambda_i)M}(-d_i)\right)\right]_l$$

By (3.1) we have that $\sigma_1([m_1]_1, \ldots, [m_{k-1}]_{k-1}, [m]_k) = 0$. Since at level l we have that $\mathrm{Ker}(\sigma_1) = \mathrm{Im}(\sigma_2)$ then there exists

$$\underset{1\leq i<j\leq k}{\oplus}[a_{ij}]_{ij} \in \left[\bigoplus_{1\leq i<j\leq k}\left(\frac{M}{(\lambda_i,\lambda_j)M}(-d_i-d_j)\right)\right]_l$$

such that

$$\sigma_2(\underset{1\leq i<j\leq k}{\oplus}[a_{ij}]_{ij}) = ([m_1]_1, \ldots, [m_{k-1}]_{k-1}, [m]_k).$$

For all $1 \leq i \leq k-1$ we have

$$\begin{aligned}[m_i]_i &= \sum_{i<p\leq k}[\lambda_p a_{ip}]_i + \sum_{1\leq q<i}[\lambda_q a_{iq}]_i \\ &= \sum_{i<p\leq k-1}[\lambda_p a_{ip}]_i + \sum_{1\leq q<i}[\lambda_q a_{iq}]_i \ + \ [\lambda_k a_{ik}]_i.\end{aligned}$$

Consider

$$\underset{1\leq i<j\leq k-1}{\oplus}[a_{ij}]_{ijk} \in \left[\bigoplus_{1\leq i<j\leq k-1}\left(\frac{M}{(\lambda_i,\lambda_j,\lambda_k)M}(-d_i-d_j)\right)\right]_l$$

Notice that

$$\overline{\delta_2}(\underset{1\leq i<j\leq k-1}{\oplus}[a_{ij}]_{ijk}) = ([y_1]_{1k}, ..., [y_{k-1}]_{(k-1)k}),$$

where

$$[y_i]_{ik} = \sum_{i<p\leq k-1}[\lambda_p a_{ip}]_{ik} + \sum_{1\leq q<i}[\lambda_q a_{iq}]_{ik}$$

Therefore, using the projection map we have that $[m_i]_{ik} = [y_i]_{ik}$ in

$(M/(\lambda_i,\lambda_k)M)(-d_i))_l$, i.e.,

$$\underset{1\leq i\leq k-1}{\oplus}[m_i]_{ik} = \overline{\delta_2}(\underset{1\leq i<j\leq k-1}{\oplus}[a_{ij}]_{ijk}).$$

It shows that $\mathrm{Ker}(\overline{\delta_1}) = \mathrm{Im}(\overline{\delta_2})$ at level l. Thus,

$$H_2(\mathcal{C}')_{<D} = 0. \tag{3.2}$$

From Proposition 3.2.8 we have that the sequence

$$H_2(\mathcal{C}'(-d_k)) \xrightarrow{\lambda_k} H_1(M \otimes \mathcal{K}(\lambda_1, ..., \lambda_{k-1})) \to H_1(M \otimes \mathcal{K}(\lambda_1, ..., \lambda_k))$$

is exact. By hypothesis and (3.2), for all $j < D$, we have that $H_1(M \otimes \mathcal{K}(\lambda_1, ..., \lambda_k))_j = 0$, and $H_2(\mathcal{C}'(-d_k))_j = 0$. By exactness of the above sequence we have that $H_1(M \otimes \mathcal{K}(\lambda_1, ..., \lambda_{k-1}))_j = 0$, for all $j < D$. □

The following theorem gives a homological characterization of the D-semi-regularity.

Theorem 3.2.10. *Let M be a non-trivial finitely generated R-module. Let $\lambda_1, ..., \lambda_m$ be a sequence of homogeneous elements of positive degrees $d_1, ..., d_m$, and let D be a natural number. Then, $\lambda_1, ..., \lambda_m$ is D-semi-regular on M if and only if $H_1(M \otimes \mathcal{K}(\lambda_1, ..., \lambda_m))_{<D} = 0$.*

Proof. Let us suppose that $\lambda_1, ..., \lambda_m$ is D-semi-regular on M. Let us prove that $H_1(M \otimes \mathcal{K}(\lambda_1, ..., \lambda_m))_{<D} = 0$ by induction on m. The induction base is $m = 1$. Let λ_1 be D-semi-regular on M. Then, by definition of D-semi-regularity we have that the sequence

$$0 \to (M/\lambda_1 M)(-d_1)_i \xrightarrow{\lambda_1} M_i \to 0$$

is exact for all $i < D$. Notice that the complex $M \otimes \mathcal{K}(\lambda_1)$ is given by

$$0 \to (M/\lambda_1 M)(-d_1) \xrightarrow{\lambda_1} M \to 0.$$

Thus, $H_1(M \otimes \mathcal{K}(\lambda_1))_{<D} = 0$. Now let $m > 1$. Since $\lambda_1, ..., \lambda_m$ is D-semi-regular on M then by definition we have that the sequence $\lambda_1, ..., \lambda_{m-1}$ is D-semi-regular on M. Consider the complexes $\mathcal{C} = M \otimes \mathcal{K}(\lambda_1, ..., \lambda_{m-1})$, $\mathcal{C} \otimes \mathcal{K}(\lambda_m) = M \otimes \mathcal{K}(\lambda_1, ..., \lambda_m)$, and $\mathcal{C}'$ as in Proposition 3.2.8. From that proposition we have that the following sequence is exact

$$H_1(M \otimes \mathcal{K}(\lambda_1, ..., \lambda_{m-1})) \to H_1(M \otimes \mathcal{K}(\lambda_1, ..., \lambda_m))$$
$$\to H_1(\mathcal{C}'(-d_m)) \xrightarrow{\lambda_m} H_0(M \otimes \mathcal{K}(\lambda_1, ..., \lambda_{m-1})).$$

Notice that $H_0(M \otimes \mathcal{K}(\lambda_1, ..., \lambda_{m-1})) = M/(\lambda_1, ..., \lambda_{m-1})M$. Now, the complex $\mathcal{C}'$ is given by

$$\mathcal{C}' : 0 \to \cdots \to \bigoplus_{1 \leq i \leq m-1} \left(\tfrac{M}{(\lambda_i, \lambda_m)M}(-d_i) \right) \xrightarrow{\overline{\delta_1}} M/\lambda_m M \to 0 \to 0$$

And by the definition of the boundary map of this complex we have that $H_1(\mathcal{C}') = (M/(\lambda_1, ..., \lambda_m)M)$. Therefore,

$$H_1(\mathcal{C}'(-d_m)) = (M/(\lambda_1, ..., \lambda_m)M)(-d_m)$$

Thus, we have the exact sequence

$$H_1(M \otimes \mathcal{K}(\lambda_1, ..., \lambda_{m-1})) \to H_1(M \otimes \mathcal{K}(\lambda_1, ..., \lambda_m))$$
$$\to (M/(\lambda_1, ..., \lambda_m)M)(-d_m) \xrightarrow{\lambda_m} M/(\lambda_1, ..., \lambda_{m-1})M.$$

By induction hypothesis we have $H_1(M \otimes \mathcal{K}(\lambda_1, ..., \lambda_{m-1}))_{<D} = 0$. Moreover, since $\lambda_1, ..., \lambda_m$ is D-semi-regular on M, then

$$((M/(\lambda_1, ..., \lambda_m)M)(-d_m))_{<D} \xrightarrow{\lambda_m} (M/(\lambda_1, ..., \lambda_{m-1})M)_{<D}$$

has trivial kernel. We conclude that $H_1(M \otimes \mathcal{K}(\lambda_1, ..., \lambda_m))_{<D} = 0$.

Conversely, let $\lambda_1, ..., \lambda_m$ be a sequence of homogeneous elements of positive degrees. Suppose that $H_1(M \otimes \mathcal{K}(\lambda_1, ..., \lambda_m))_{<D} = 0$. By Lemma 3.2.9 we have that $H_1(M \otimes \mathcal{K}(\lambda_1, ..., \lambda_k))_{<D} = 0$, for all $k = 1, ..., m$. As above, we have that the sequence

$$H_1(M \otimes \mathcal{K}(\lambda_1, ..., \lambda_k)) \to (M/(\lambda_1, ..., \lambda_k)M)(-d_k) \xrightarrow{\lambda_k} M/(\lambda_1, ..., \lambda_{k-1})M$$

is exact for all $k = 1, ..., m$. Since $H_1(M \otimes \mathcal{K}(\lambda_1, ..., \lambda_k))_{<D} = 0$, for all $k = 1, ..., m$, then the kernel of the map

$$((M/(\lambda_1, ..., \lambda_k)M)(-d_k))_{<D} \xrightarrow{\lambda_k} (M/(\lambda_1, ..., \lambda_{k-1})M)_{<D}$$

is trivial for all $k = 1, ..., m$. Therefore $\lambda_1, ..., \lambda_m$ is D-semi-regular on M. $\square$

3.3 Relation between Semi-Regularity and Semi-Regularity over $\mathbb{F}_2$

Let $S^{(n)} = \mathbb{F}_2[X_1, ..., X_n]$ be the ring of polynomials in n-variables over the field $\mathbb{F}_2$. Let $B^{(n)} = \mathbb{F}_2[X_1, ..., X_n]/(X_1^2, ..., X_n^2)$. Denote the image of X_i in $B^{(n)}$ by x_i. Given $g \in B^{(n)}$ let us denote by g' the natural lifting of g in $S^{(n)}$. In other words, if $g(x_1, \ldots, x_n)$ is a polynomial in $B^{(n)}$ then the natural lifting of g in $S^{(n)}$ is the polynomial g' obtained from g by replacing each occurrence of x_i in g by X_i. Thus, $g' = g(X_1, \ldots, X_n) \in S^{(n)}$.

The natural question that could be asked is the following: Given a sequence of homogeneous polynomials $\lambda_1, \ldots, \lambda_m$ in $B^{(n)}$ what is the relation between the semi-regularity of the sequence $\lambda_1, \ldots, \lambda_m$ in $B^{(n)}$ and the semi-regularity of the sequence $X_1^2, ..., X_n^2, \lambda_1', ..., \lambda_m'$ in $S^{(n)}$? The next theorem and example show how these two concepts are related.

Theorem 3.3.1. *Let $\lambda_1, ..., \lambda_m$ be a sequence of homogeneous elements in $B^{(n)}$ where $\deg(\lambda_i) = d_i$. If $X_1^2, ..., X_n^2, \lambda_1', ..., \lambda_m'$ is semi-regular on $S^{(n)}$ then $\lambda_1, ..., \lambda_m$ is semi-regular on $B^{(n)}$.*

Proof. Let $I = (X_1^2, ..., X_n^2, \lambda_1', ..., \lambda_m') \subset S^{(n)}$ and $J = (\lambda_1, ..., \lambda_m) \subset B^{(n)}$. Note that

$$S^{(n)}/I \cong B^{(n)}/J.$$

Therefore, $\mathrm{Ind}(I) = \mathrm{Ind}(J)$. Let $g \in B^{(n)}$ such that $g\lambda_i \in (\lambda_1, ..., \lambda_{i-1}) \subset B^{(n)}$ and $\deg(g) + \deg(\lambda_i) < \mathrm{Ind}(J)$. Thus, $g'\lambda_i' \in (X_1^2, ..., X_n^2, \lambda_1', ..., \lambda_{i-1}') \subset S^{(n)}$ and $\deg(g') + \deg(\lambda_i') < \mathrm{Ind}(I)$. Since $X_1^2, ..., X_n^2, \lambda_1', ..., \lambda_m'$ is semi-regular on $S^{(n)}$, we have that $g' \in (X_1^2, ..., X_n^2, \lambda_1', ..., \lambda_{i-1}') \subset (X_1^2, ..., X_n^2, \lambda_1', ..., \lambda_{i-1}', \lambda_i') \subset S^{(n)}$ therefore $g \in (\lambda_1, ..., \lambda_i) \subset B^{(n)}$. □

However, $\lambda_1, ..., \lambda_m$ semi- regular on $B^{(n)}$ does not imply that $X_1^2, ..., X_n^2, \lambda_1', ..., \lambda_m'$ is semi-regular on $S^{(n)}$ as the following example shows.

Example 2. Let $f = \sum_{1 \leq i < j \leq n} x_i x_j \in B^{(n)}$, $I = (X_1^2, ..., X_n^2, f') \subset S^{(n)}$, $J = (f) \subset B^{(n)}$. Consider

$$\begin{aligned} h(z) &= \mathrm{HS}_I(z) \\ g(z) &= \left[(1+z)^n/(1+z^2)\right] \\ l(z) &= \left[(1-z^2)^{n+1}/(1-z)^n\right] \end{aligned}$$

When $n = 6$ we have that

$$\begin{aligned} h(z) &= 1 + 6z + 14z^2 + 14z^3 + z^4 \\ g(z) &= 1 + 6z + 14z^2 + 14z^3 + z^4 \\ l(z) &= 1 + 6z + 14z^2 + 14z^3 \end{aligned}$$

By Theorem 3.2.6 and Theorem 3.1.3 we have that f is semi-regular on $B^{(n)}$ but the sequence $X_1^2, ..., X_6^2, f'$ is not semi-regular on $S^{(n)}$.

In Section 4.2.4 we present more results about the semi-regularity of the sequence $X_1^2, ..., X_n^2, f'$ on $S^{(n)}$, where f is the natural lifting of a homogeneous element $f \in B^{(n)}$.

On the other side, one of the simplest and most important cases of study of sequences of polynomials in cryptography, is that of quadratic sequences of length n in n variables over the field $\mathbb{F}_2$. Thus, a natural question is: Why given a sequence $f_1, \ldots, f_n \in B^{(n)}$ should we study the semi-regularity over $B^{(n)}$ rather than the semi-regularity of the sequence $X_1^2, \ldots, X_n^2, f_1', \ldots, f_n'$ over the ring $S^{(n)}$? We will show that given a sequence of homogeneous quadratic polynomials $f_1, \ldots, f_n \in B^{(n)}$, the sequence $X_1^2, \ldots, X_n^2, f_1', \ldots, f_n' \in S^{(n)}$ is never semi-regular over the ring $S^{(n)}$ for $n \geq 16$. While, as we will see in Section 4.1, it is conjectured that the proportion $\pi(n, n, 2)$ of sequences of quadratic elements of length n in $B^{(n)}$ that are semi-regular tends to 1 as n goes to infinity. Therefore, given a sequence of homogeneous polynomials $\lambda_1, \ldots, \lambda_m$ in $B^{(n)}$ the notion of semi-regularity over $\mathbb{F}_2$ given

in Section 3.2 is a more suitable notion than the one of semi-regularity of the sequence $X_1^2, ..., X_n^2, \lambda'_1, ..., \lambda'_m$ in $S^{(n)}$ given in Section 3.1.

Let us define

$$S_n(z) = \frac{(1-z^2)^{2n}}{(1-z)^n} = (1+z)^n(1-z^2)^n$$

and

$$T_n(z) = \frac{(1+z)^n}{(1+z^2)^n} = (1+z)^n \left(\sum_{i=0}^{\infty} (-1)^i z^{2i} \right)$$

Let $a(z) = \sum_i a_i z^i \in \mathbb{R}[[z]]$. By the product of two power series we have that

$$\left(\sum a_k z^k \right) (1-z^d)^m = \sum b_k z^k \tag{3.3}$$

where $b_k = \sum_{i=0}^{\lfloor k/d \rfloor} (-1)^i \binom{n}{i} a_{k-di}$.

Lemma 3.3.2. $\operatorname{Ind} S_n(z) \geq 5$ *for all* $n \geq 16$.

Proof. Consider $\sum b_k z^k = S_n(z) = (1+z)^n(1-z^2)^n$. By (3.3) we have that $b_0 = 1$, $b_1 = n$, $b_2 = \binom{n}{2} - n$, $b_3 = \binom{n}{3} - n^2$ and $b_4 = \binom{n}{4} + \binom{n}{2}(1-n)$. Let us see that $b_4 > 0$ for all $n \geq 16$. We have that

$$b_4 = \frac{n(n-1)(n-2)(n-3)}{4!} - \frac{n(n-1)^2}{2!}$$

Thus, $b_4 > 0$ if and only if $n(n-1)(n-2)(n-3) - 12n(n-1)^2 > 0$ or equivalently, if and only if $n(n-1)\{(n-2)(n-3) - 12(n-1)\} > 0$. It is easily seen that $(n-2)(n-3) - 12(n-1) > 0$ for all $n \geq 16$. Thus, $b_4 > 0$ for all $n \geq 16$. In a similar way we can see that for all $n \geq 16$ we have that $b_i > 0$ for $i = 2, 3$. □

Lemma 3.3.3. *Let* $S_n(z) = \sum b_k z^k$ *and* $T_n(z) = \sum c_k z^k$. *Then for* $n \geq 5$ *we have that* $c_4 = b_4 + n$ *and* $c_i = b_i$ *for* $i = 0, \ldots, 3$.

Proof. By Lemma 3.2.5 we have that

$$\begin{aligned}
[T]_5 &= \left[(1+z)^n \left(\sum_{i=0}^{\infty}(-1)^i z^{2i}\right)\right]_5 \\
&= \left[(1+z)^n \left[\sum_{i=0}^{\infty}(-1)^i z^{2i}\right]_5\right]_5 \\
&= [(1+z)^n(1-z^2+z^4)^n]_5
\end{aligned}$$

Thus,

$$\begin{aligned}
[T]_5 &= \left[(1+z)^n \left(\sum_{i=0}^{n}\binom{n}{i}(1-z^2)^{n-i}(z^4)^i\right)\right]_5 \\
&= \left[(1+z)^n \left[\sum_{i=0}^{n}\binom{n}{i}(1-z^2)^{n-i}(z^4)^i\right]_5\right]_5 \\
&= [(1+z)^n((1-z^2)^n + n(z^4)(1-z^2)^{n-1})]_5 \\
&= [(1+z)^n((1-z^2)^n + [n(z^4)(1-z^2)^{n-1}]_5)]_5 \\
&= [(1+z)^n((1-z^2)^n + n(z^4))]_5 \\
&= [(1+z)^n(1-z^2)^n + (1+z)^n n(z^4))]_5 \\
&= [S_n(z) + (1+z)^n n(z^4))]_5
\end{aligned}$$

Therefore,

$$[T]_5 = b_0 + b_1 z + b_2 z^2 + b_3 z^3 + b_4 z^4 + nz^4$$

as we needed to show. □

Theorem 3.3.4. *Let $n \geq 16$ and let $g_1, \ldots, g_n \in S^{(n)}$ be a sequence of homogeneous quadratic polynomials. Then, the sequence $X_1^2, \ldots, X_n^2, g_1, \ldots, g_n \in S^{(n)}$ is not semi-regular over the ring $S^{(n)}$.*

Proof. Let $n \geq 16$, let $g_1, \ldots, g_n \in S^{(n)}$ be a sequence of homogeneous quadratic polynomials and let L be the ideal generated by the sequence $X_1^2, ..., X_n^2, g_1, ..., g_n$. Notice that $d_{reg}(L) = \min\{d \geq 0 \mid L \cap S_d = S_d\} > 2$ since $n \geq 16$. Consider f_i as the image of the polynomial g_i under the evaluation map

$$\mathbb{F}_2[X_1, ..., X_n] \to B^{(n)}$$

$$X_i \mapsto x_i$$

If $f_i = 0$ for some i, then $g_i \in (X_1^2, \ldots, X_n^2, g_1, \ldots, g_{i-1})$ and $\deg 1 + \deg g_i = 2 < d_{reg}(L)$. However, $1 \notin (X_1^2, \ldots, X_n^2, g_1, \ldots, g_{i-1})$, therefore the sequence $X_1^2, ..., X_n^2, g_1, ..., g_n$ cannot be semi-regular on $S^{(n)}$. Now, let us suppose that $f_i \neq 0$ for all $i = 0, \ldots, n$. Consider f_i' the natural lifting of f_i in $S^{(n)}$. Note that the ideals $I = (X_1^2, ..., X_n^2, f_1', ..., f_n')$ and $L = (X_1^2, ..., X_n^2, g_1, ..., g_n)$ are the same ideal in the ring $S^{(n)}$. By Theorem 3.1.3 we have that the sequence $X_1^2, ..., X_n^2, g_1, ..., g_n$ is semi-regular if and only if the sequence $X_1^2, ..., X_n^2, f_1', ..., f_n'$ is semi-regular. Suppose that the sequence $X_1^2, \ldots, X_n^2, f_1', \ldots, f_n'$ is semi-regular over $S^{(n)}$. By Theorem 3.3.1 we have that $f_1, \ldots, f_n$ is semi-regular on $B^{(n)}$. Let $J = (f_1, ..., f_n) \subset B^{(n)}$. By Theorem 3.1.3 and Theorem 3.2.6 we have that

$$[S_n(z)] = \left[\frac{(1-z^2)^{2n}}{(1-z)^n}\right] = \mathrm{HS}_{S^{(n)}/I} = \mathrm{HS}_{B^{(n)}/J} = \left[\frac{(1+z)^n}{(1+z^2)^n}\right] = [T_n(z)].$$

But by Lemma 3.3.2 and Lemma 3.3.3 this is not possible. □

CHAPTER 4

On the Existence of Semi-Regular Sequences over $\mathbb{F}_2$

4.1 Conjectures and Questions on Semi-Regularity

It has been conjectured that randomly generated sequences tend to be semi-regular [4, Section 3]. However very little progress has been made towards proving this conjecture. In fact even the question of the existence of semi-regular quadratic sequences of length n in n of variables remains open. Let us begin by reviewing some of the conjectures made by Bardet et al.

Conjecture 1. [3, 6] The proportion of semi-regular sequences tends to one as the number of variables tends to infinity.

Notice that this conjecture is ambiguous in the sense that it is not defined precisely the meaning of " proportion of semi-regular sequences". If the proportion of semi-regular sequences in the ring $B^{(n)}$ is interpreted as the quotient $s(n)/h(n)$ where $h(n)$ is the number of subsets of $B^{(n)}$ consisting of homogeneous elements of degree greater than or equal to one and $s(n)$ is the number of such subsets that are semi-regular then the conjecture was proved to be true by J. Schlather. He proved that

$$\lim_{n\to\infty} \frac{s(n)}{h(n)} = 1$$

Unfortunately this result does not give us the kind of information that we are interested in. As the size of the set increases, so does the likelihood of it being semi-regular for trivial reasons (for instance any basis of the set of quadratic polynomials is trivially semi-regular). J. Schlather showed that the proportion of sequences that are trivially semi-regular tends to one.

A different formulation of the conjecture about that "most" sequences are semi-regular is given in [4, Conjecture 2]

Conjecture 2. [4] For any $(n, m, d_1, \ldots, d_m)$ the proportion $\pi(n, m, d_1, \ldots, d_m)$ of semi-regular sequences over $\mathbb{F}_2$ in the set $E(n, m, d_1, \ldots, d_m)$ of algebraic systems of m equations of degrees $d_1, \ldots, d_m$ in n variables tends to 1 as n tends to ∞.

Notice that this conjecture is also ambiguous in the sense that it is not stated whether or not the variables length of the sequence m and number of variables n are related in some way (for example if m is a function of n). In Section 4.4, I show in Theorem 4.4.14 that for a fixed choice of $(m, d_1, \ldots, d_m)$, we have that

$$\lim_{n\to\infty} \pi(n, m, d_1, \ldots, d_m) = 0.$$

Neither of these conjectures accurately addresses the observed fact that "most" quadratic sequences of length n in n variables are semi-regular. More generally we make the following conjecture.

Conjecture 3. For any $1 \leq d \leq n$ define $\pi(n, d)$ to be the proportion of sequences of degree d and length n in n variables that are semi-regular. Then

$$\lim_{n\to\infty} \pi(n, d) = 1.$$

In fact we expect much more to be true. Define $\pi(n, m, d)$ to be the proportion of sequences of degree d and length m in n variables that are semi-regular. The Table 4.1 below

presents some data about the following experiment that I performed: Notice that the dimension of the set of quadratic homogeneous polynomials in $B^{(n)}$ is $\dim B_2^{(n)} = \binom{n}{2}$. Note that each element in $B_2^{(n)}$ is just a linear combination over $\mathbb{F}_2$ of quadratic monomials. Thus, I "randomly" selected (using the random generator function from the computer program *Magma*) a number in the set $\{0, 1\}$ to get coefficients for each of the quadratic monomials in $B^{(n)}$ and eventually getting a set consisting of 20 subsets, each subset consisting of m quadratic homogeneous polynomials in n variables. The term "set" used here is the one used in mathematics, there cannot be repeated elements. For each subset of m quadratic polynomials in $B^{(n)}$, constructed above, let us say $\{\lambda_1, \ldots, \lambda_m\}$, using the function to calculate Hilbert Series implemented in *Magma*, I checked whether or not the equality

$$\mathrm{HS}_{B^{(n)}/(\lambda_1,\ldots,\lambda_m)}(z) = \left[\frac{(1+z)^n}{(1+z^2)^m}\right]$$

was satisfied (remember the Hilbert Characterization of semi-regular sequences presented in Section 3.2.1). If the equality was satisfied then the sequence $\lambda_1, \ldots, \lambda_m$ was semi-regular, if not, the sequence was not semi-regular. This allowed me to calculate the proportion of this sets that were semi-regular. For instance, in the table we have that for $n = 5$ and $m = 3$ the corresponding entry is 0.85, meaning that 85% of the 20 sets of 3 quadratics in 5 variables were semi-regular. I could not perform the experiment when the number of variables n was 16 since the memory of my computer was exhausted.

Theorem 4.4.14 states that all columns of Table 1 eventually become zero. We conjecture that the non-zero entries of the rows tend to one as $n \to \infty$. One formulation of this is the following conjecture.

$n\backslash m$	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3	1	.8	1	1	1	1								
4	.7	1	.75	.75	.3	.65	.85	.9	1	1	1	1	1	1
5	0	.85	.95	1	.9	.85	.75	.6	.2	.65	.9	.9	.9	0.95
6	.85	.7	.65	.9	1	1	1	.95	.95	.95	.75	.8	.5	.25
7	0	.85	1	.1	1	1	1	1	1	1	1	.95	1	1
8	.7	.45	1	1	.95	.1	1	1	1	1	1	1	1	1
9	0	.95	.7	1	1	1	1	.8	.9	1	1	1	1	1
10	0	.85	1	.35	1	1	1	1	1	1	.25	1	1	1
11	0	.95	1	1	1	1	1	1	1	1	1	1	1	.4
12	0	0	1	1	1	1	.9	1	1	1	1	1	1	1
13	0	0	1	1	1	1	1	1	1	1	1	1	1	1
14	0	0	0	1	1	1	1	1	1	1	1	1	1	1
15	0	0	0	1	1	1	1	1	1	1	1	1	.45	1

Table 4.1: Proportion of Samples of 20 Sets of m Homogeneous Quadratic Elements in n variables that are Semi-Regular

Conjecture 4. Fix $d > 1$. Define $\pi(n, m, d)$ to be the proportion of sequences of degree d and length m in n variables that are semi-regular. Then there exists an $0 < \eta_d \leq 1/3$ such that for all $\epsilon > 0$, there exists an $N > 0$ such that

$$\pi(n, m, d) > 1 - \epsilon \text{ for all } n > N \text{ and all } m > \eta_d N.$$

While we believe these conjectures to be true, it should be noted that the existence question still remains largely open.

Question 1. For which pairs $(n, \mathbf{d} = (d_1, \ldots, d_m))$ do there exist semi-regular sequences $\lambda_1, \ldots, \lambda_m$ with $\deg \lambda_i = d_i$?

At both ends of the degree spectrum, the existence question is trivial. Sequences of linear elements are semi-regular if and only if they are linearly independent. Likewise for sequences of degree $n - 1$ (and n). Also for sufficiently large m it is easy to find sequences that are trivially semi-regular; for instance a basis of the space of polynomials of degree d.

4.2 The case $m = 1$: semi-regularity of homogeneous polynomials

4.2.1 Non-semi-regularity of a homogeneous polynomial

In this section we review some results of J. Schlather and T. Hodges about semi-regularity in the case when the polynomial is linear or quadratic. Also, it is shown that the proportion of semi-regular elements of degree d in $B^{(n)}$ is zero when $n > 3d$.

Proposition 4.2.1. *Let $\lambda \in B_1^{(n)}$ then λ is semi-regular and* $\mathrm{Ind}(\lambda) = n$.

Proof. Without loss of generality we can assume that

$$\lambda = x_1 \in B^{(n)}.$$

In this case $B^{(n)}/(x_1) \cong B^{(n-1)}$ which has Hilbert series $(1+z)^{n-1}$. On the other hand $T_{(1),n}(z) = (1+z)^n/(1+z) = (1+z)^{n-1}$. So by Theorem 3.2.6, this element is semi-regular and $\mathrm{Ind}(\lambda) = n$. □

Theorem 4.2.2. *Let $\lambda \in B^{(n)}$ be homogeneous of degree d. If $d = n$ or $d = n-1$ then λ is semi-regular .*

Proof. Let $\lambda \in B^{(n)}$ be homogeneous of degree d, with $n-1 \leq d \leq n$. Note that $\mathrm{Ind}(\lambda) = n$. The semi-regularity of λ follows trivially from the definition. □

Lemma 4.2.3. *Let $\lambda \in B^{(n)}$ be a monomial then* $\mathrm{Ann}\,\lambda = (\mathrm{var}(\lambda))$ *where* $\mathrm{var}(\lambda)$ *is the set of variables occurring in λ.*

Proof. The inclusion $(\mathrm{var}(\lambda)) \subset \mathrm{Ann}\,\lambda$ is clear. Let $\nu \in \mathrm{Ann}\,\lambda$ and write $\nu = \nu_1 + \cdots + \nu_r$, where the ν_i are distinct monomials. Since λ is a monomial then for $i \neq j$ it follows that $\nu_i\lambda \neq \nu_j\lambda$ unless $\nu_i\lambda = \nu_j\lambda = 0$. Thus, since $\lambda\nu = 0$ then $\lambda\nu_j = 0$ for all $j = 1, \ldots, r$. Therefore, for all $j = 1, \ldots, r$ we have that λ and ν_j must share some x_i. Hence $\nu \in (\mathrm{var}(\lambda))$. □

Definition 4.2.4. Let $\lambda \in B^{(n)}$ be a homogeneous polynomial of degree d. λ can be written in the form

$$\lambda = \sum_{m \in \mu_d} \epsilon_m m,$$

where μ_d is the set of monomials of degree d, and ϵ_m is either 1 or 0. The *support* of λ is defined as

$$\mathrm{Supp}(\lambda) = \{m \mid \epsilon_m = 1\}.$$

Proposition 4.2.5. *Let $\lambda \in B^{(n)}$ be homogeneous of degree d. Then* $\mathrm{Ind}(\lambda) > n - d$.

Proof. By renumbering we may assume $x_1 \cdots x_d \in \mathrm{Supp}(\lambda)$. We demonstrate $x_{d+1} \cdots x_n \notin (\lambda)$. Suppose for the sake of contradiction that we have $\nu \in B^{(n)}_{n-2d}$ such that $\nu\lambda = x_{d+1} \cdots x_n$. Writing ν and λ as polynomials in x_1, i.e. $\lambda = x_1\lambda_1 + \lambda_0$ and $\nu = x_1\nu_1 + \nu_0$ then

$$\lambda_0\nu_0 + x_1(\lambda_1\nu_0 + \lambda_0\nu_1) = x_{d+1} \cdots x_n.$$

So $\lambda_1\nu_0 + \lambda_0\nu_1 \in \mathrm{Ann}\, x_1$, but $x_1 \notin \mathrm{var}(\lambda_1\nu_0 + \lambda_0\nu_1)$ therefore $\lambda_1\nu_0 = \lambda_0\nu_1$. In particular

$$x_{d+1} \cdots x_n\lambda_1 = \lambda_0\nu_0\lambda_1 = \lambda_0^2\nu_1 = 0,$$

so $\lambda_1 \in \mathrm{Ann}\, x_{d+1} \cdots x_n = (x_{d+1}, \cdots, x_n)$ but $x_2 \cdots x_d \in \mathrm{Supp}\, \lambda_1$, which is impossible. □

Now, we will use a result that appears in [25] about the *first fall degree* of a homogeneous polynomial $\lambda \in B^{(n)}$. Basically, the first fall degree of λ, denoted by $\mathrm{D_{ff}}(\lambda)$, is the first degree at which non-trivial relations occur; the trivial relations being relations such as $g\lambda = 0$ where $g \in (\lambda)$. In other words the first fall degree of λ is the first k such that there exists g in $B^{(n)}$ with the property that $\deg g + \deg \lambda = k$, $g\lambda = 0$ and $g \notin (\lambda)$. In [25] the authors give a more detailed and general definition for the first fall degree.

Definition 4.2.6. Let λ be a homogeneous element of $B^{(n)}$. The *rank* of λ is the smallest integer s such that there exist $\mu_1, \ldots, \mu_s \in B^{(n)}_1$ with $\lambda \in \mathbb{F}_2[\mu_1, \ldots, \mu_s]$. That is, s is the smallest number of linear elements required to generate λ.

Theorem 4.2.7. *Let λ be an element of degree $d > 1$ and rank s. Then* $\mathrm{D_{ff}}(\lambda) \leq (s+d+2)/2$.

Proof. See Theorem 4.9 in [25]. □

This enables us to give a result on the non-existence of semi-regular elements of degree $d \geq 2$ when $n > 3d$.

Theorem 4.2.8. *Let $\lambda_1, \ldots, \lambda_m$ be a sequence of homogeneous polynomials of degrees $d_1, \ldots, d_m$ in $B^{(n)}$. If* $\mathrm{Ind}(\lambda_1, \ldots, \lambda_m) > \mathrm{D_{ff}}(\lambda_i)$ *for some $1 \leq i \leq m$ then $\lambda_1, \ldots, \lambda_m$ is not semi-regular.*

Proof. Suppose $\lambda_1, \ldots, \lambda_m$ is a sequence of homogeneous polynomials such that $\mathrm{Ind}(\lambda_1, \ldots, \lambda_m) > \mathrm{D_{ff}}(\lambda_i)$ for some $1 \leq i \leq m$. If $\lambda_1, \ldots, \lambda_m$ is a semi-regular sequence then by Theorem 3.2.6 any reordering of this sequence is also a semi-regular sequence. Thus, without loss of generality we can assume that $\mathrm{Ind}(\lambda_1, \ldots, \lambda_m) > \mathrm{D_{ff}}(\lambda_1)$. By definition of first fall degree there exists g such that $g\lambda_1 = 0$, $\deg g + \deg \lambda_1 = \mathrm{D_{ff}}(\lambda_1) < \mathrm{Ind}(\lambda_1, \ldots, \lambda_m)$ and $g \notin (\lambda_1)$. But it is not possible if $\lambda_1, \ldots, \lambda_m$ is semi-regular. Therefore $\lambda_1, \ldots, \lambda_m$ cannot be semi-regular. □

Corollary 4.2.9. *Let λ be homogeneous. If* $\mathrm{Ind}(\lambda) > \mathrm{D_{ff}}(\lambda)$ *then λ is not semi-regular.*

Theorem 4.2.10. *There are no semi-regular elements of degree $d \geq 2$ for $n > 3d$.*

Proof. Let λ be a homogeneous element with $\deg \lambda = d > 1$ and suppose that $n > 3d$. Then $(n + d)/2 < n - d$. Since the rank s of λ is less than or equal to n, we have by Theorem 4.2.7 and Proposition 4.2.5 that

$$\mathrm{D_{ff}}(\lambda) \leq \frac{s+d+2}{2} \leq \frac{n+d+2}{2} < n - d + 1 \leq \mathrm{Ind}(\lambda).$$

Since the first fall degree of λ is less than its index it cannot be semi-regular. □

Remark 1. Let λ be a homogeneous element in $B^{(n)}$. If we want to know if this element is semi-regular it is enough to compute its Hilbert series (Theorem 3.2.6). The Hilbert series of λ depends only of the dimension of $\lambda B_k^{(n)}$, and these dimensions are obviously invariant

under any automorphism that preserves degree. Inside the group of all automorphisms of $B^{(n)}$ we have the group of automorphisms that preserve degree; that is, the subgroup of all automorphism ϕ such that $\phi(B_1^{(n)}) = B_1^{(n)}$. Notice this group of automorphisms is isomorphic to $GL_n(\mathbb{F}_2)$. We say that two elements $\lambda, \lambda' \in B^{(n)}$ are equivalent if there exists an automorphism of $B^{(n)}$ such ϕ such that $\phi(\lambda) = \lambda'$ and $\phi(B_1^{(n)}) = B_1^{(n)}$. Thus, given two equivalent homogeneous elements λ, λ' we have that λ is semi-regular if and only if λ' is semi-regular.

The next theorem uses the above remark and the classification of quadratic elements in the polynomial given [29] to give a complete description of the proportion of quadratic semi-regular elements.

Theorem 4.2.11. *There are no semi-regular elements of degree 2 for $n \geq 7$. That is, $\pi(n, 1, 2) = 0$ for $n \geq 7$. For $2 \leq n \leq 6$ the value of $\pi(n, 1, 2)$ is given by the table*

n	2	3	4	5	6
$\pi(n, 1, 2)$	1	1	28/63	868/1023	13,888/32,767

Proof. The first part is just a consequence of Theorem 4.2.10.

Let us consider the cases $n = 2, \ldots, 6$. By the above remark and by the classification of quadratic elements given in [29] we just need to compute the Hilbert series of a polynomial of a given rank using the specific case of $x_1x_2, x_1x_2 + x_3x_4$ and $x_1x_2 + x_3x_4 + x_5x_6$. The cases $n = 2$ and 3 follow from Theorem 4.2.2. When $n = 4$ the Hilbert series of a rank two element is $1 + 4z + 5z^2 + 2z^3$ and that of a rank 4 element is $1 + 4z + 5z^2$ which is $[T_{(2),4}(z)]$. Thus, the rank four elements are semi-regular and the rank two elements are not. Let us calculate the number of elements of rank two in $B_2^{(4)}$. Consider $G = GL_4(\mathbb{F}_2)$ acting on $B_2^{(4)}$. By the counting formula we have that $|G| = |Stab_G(x_1x_2)||\mathcal{O}_G(x_1x_2)|$, where $Stab_G(x_1x_2)$ denotes the stabilizer of x_1x_2 under the action of G and $\mathcal{O}_G(x_1x_2)$ denotes the orbit of of x_1x_2 under

the action of G. Thus, $|\mathcal{O}_G(x_1x_2)|$ is the number of elements rank two in $B_2^{(4)}$. Notice that $|G| = (2^4-1)(2^4-2)(2^4-2^2)(2^4-2^3)$. On the other side, any element in $Stab_G(x_1x_2)$ is of the form

$$\begin{bmatrix} A & B \\ O & C \end{bmatrix}$$

with $A, C \in GL_2(\mathbb{F}_2)$, B is any matrix 2×2 with coefficients in $\mathbb{F}_2$ and O is the null matrix 2×2. Thus, $|Stab_G(x_1x_2)| = |GL_2(\mathbb{F}_2)|^2(2^4) = 3^2 \cdot 2^6$. Then, the number of quadratic homogeneous elements of rank two is $|G|/|Stab_G(x_1x_2)| = 35$. Note that the number of quadratic homogeneous elements is $|B_2^{(4)} \setminus \{0\}| = 2^6 - 1 = 63$. Therefore, there are 28 quadratic homogeneous elements of rank four and 35 elements of rank two. Thus, the proportion of semi-regular elements is $28/63 \approx 0.444$. In the case $n = 5$, the Hilbert series of a rank two element is $1 + 5z + 9z^2 + 7z^3 + 2z^4$ and that of a rank 4 element is $1 + 5z + 9z^2 + 5z^3 = [T_{(2),5}(z)]$. Thus, the rank four elements are semi-regular and the rank two elements are not. Let us calculate the number of elements of rank two in $B_2^{(5)}$. Consider $G = GL_5(\mathbb{F}_2)$ acting on $B_2^{(5)}$. By the counting formula we have that $|G| = |Stab_G(x_1x_2)||\mathcal{O}_G(x_1x_2)|$. Thus, $|\mathcal{O}_G(x_1x_2)|$ is the number of elements rank two in $B_2^{(5)}$. Notice that $|G| = (2^5-1)(2^5-2)(2^5-2^2)(2^5-2^3)(2^5-2^4)$. On the other side, any element in $Stab_G(x_1x_2)$ is of the form

$$\begin{bmatrix} A & B \\ O & C \end{bmatrix}$$

with $A \in GL_2(\mathbb{F}_2)$, $C \in GL_3(\mathbb{F}_2)$, B is any matrix 2×3 with coefficients in $\mathbb{F}_2$ and O is the null matrix 3×2. Thus, $|Stab_G(x_1x_2)| = |GL_2(\mathbb{F}_2)||GL_3(\mathbb{F}_2)|(2^6) = 2^{10} \cdot 3^2 \cdot 7$. Then, the number of quadratic homogeneous elements of rank two is $|G|/|Stab_G(x_1x_2)| = 155$. Note that the number of quadratic homogeneous elements is $|B_2^{(5)} \setminus \{0\}| = 2^{10} - 1 = 1023$. Therefore, there are 868 quadratic homogeneous elements of rank four and 155 elements of rank two. Thus, the proportion of semi-regular elements is $868/1023 \approx 0.8484$. When

$n = 6$ the Hilbert series of a rank two element is $1 + 6z + 14z^2 + 16z^3 + 9z^4 + 2z^5$, that of a rank 4 element is $1 + 6z + 14z^2 + 14z^3 + 5z^4$ and that of a rank six element is $1 + 6z + 14z^2 + 14z^3 + z^4 = [T_{(2),6}(z)]$. Thus, the rank six elements are semi-regular and the rank two and rank four elements are not. Let us calculate the number of elements of rank two in $B_2^{(6)}$. Consider $G = GL_6(\mathbb{F}_2)$ acting on $B_2^{(6)}$. By the counting formula we have that $|G| = |Stab_G(x_1x_2)||\mathcal{O}_G(x_1x_2)|$. Thus, $|\mathcal{O}_G(x_1x_2)|$ is the number of elements rank two in $B_2^{(6)}$. Notice that $|G| = (2^6-1)(2^6-2)(2^6-2^2)(2^6-2^3)(2^6-2^4)(2^6-2^5)$. On the other side, any element in $Stab_G(x_1x_2)$ is of the form

$$\begin{bmatrix} A & B \\ O & C \end{bmatrix}$$

with $A \in GL_2(\mathbb{F}_2)$, $C \in GL_4(\mathbb{F}_2)$, B is any matrix 2×4 with coefficients in $\mathbb{F}_2$ and O is the null matrix 4×2. Thus, $|Stab_G(x_1x_2)| = |GL_2(\mathbb{F}_2)||GL_4(\mathbb{F}_2)|(2^8) = 2^{15} \cdot 3^3 \cdot 5 \cdot 7$. Then, the number of quadratic homogeneous elements of rank two is $|G|/|Stab_G(x_1x_2)| = 651$. Consider $G' = GL_4(\mathbb{F}_2)$. Note that any element in $Stab_G(x_1x_2 + x_3x_4)$ is of the form

$$\begin{bmatrix} A & B \\ O & C \end{bmatrix}$$

where $A \in Stab_{G'}(x_1x_2 + x_3x_4)$, $C \in GL_2(\mathbb{F}_2)$, B is any matrix 4×2 with coefficients in $\mathbb{F}_2$ and O is the null matrix 2×4. From the case $n = 4$ we know that $|\mathcal{O}_{G'}(x_1x_2 + x_3x_4)| = 28$. Thus, $|Stab_{G'}(x_1x_2 + x_3x_4)| = G'/|\mathcal{O}_{G'}(x_1x_2 + x_3x_4)| = 2^4 \cdot 3^2 \cdot 5$. Therefore, $|Stab_G(x_1x_2 + x_3x_4)| = |Stab_{G'}(x_1x_2 + x_3x_4)||GL_2(\mathbb{F}_2)|(2^8) = 2^{13} \cdot 3^3 \cdot 5$. Then, the number of quadratic homogeneous elements of rank four is $|G|/|Stab_G(x_1x_2 + x_3x_4)| = 2^2 \cdot 3 \cdot 7^2 \cdot 31 = 18,228$. Note that the number of quadratic homogeneous elements is $|B_2^{(6)} \setminus \{0\}| = 2^{15} - 1 = 32,767$. Therefore, there are 651 quadratic homogeneous elements of rank two, $18,228$ elements of rank four and $13,888$ elements of rank six. Thus, the proportion of semi-regular elements is $13,888/32,767 \approx 0.4238$. □

In her thesis [3], Bardet asserts that the element $\sum_{1\leq i<j\leq n} x_i x_j$ is semi-regular for all n over $\mathbb{F}_2$. It was observed in [26, Lemma 3.12], that there are no quadratic semi-regular elements when $n > 6$.

Theorem 4.2.10 tells us that there are no semi-regular elements of degree $d \geq 2$ for $n > 3d$. We consider the case of a single homogeneous element of arbitrary degree $d \leq n/3$. The Table 4.2.1 below gives some data about the following experiment: Notice that the dimension of the set of homogeneous polynomials of degree d in $B^{(n)}$ is $\dim B_d^{(n)} = \binom{n}{d}$. Note that each element in $B_d^{(n)}$ is just a linear combination over $\mathbb{F}_2$ of monomials of degree d. Thus, I "randomly" selected (using the random generator function from the computer program *Magma*) a number in the set $\{0, 1\}$ to get coefficients for each of the monomials of degree d in $B^{(n)}$, eventually getting a set consisting of 20 different homogeneous elements of degree d in $B^{(n)}$. For each homogeneous element of degree d in $B^{(n)}$, constructed above, let us say λ, using the function to calculate Hilbert Series implemented in *Magma*, I checked whether or not the equality

$$\mathrm{HS}_{B^{(n)}/(\lambda)}(z) = \left[\frac{(1+z)^n}{(1+z^d)}\right]$$

was satisfied (remember the Hilbert Characterization of semi-regular sequences presented in Section 3.2.1). If the equality was satisfied then the element λ was semi-regular, if not, the element was not semi-regular. This allowed me to calculate the proportion of this elements that were semi-regular. For instance, in the table we have that for $n = 6$ and $d = 4$ the corresponding entry is 0.45, meaning that 45% of the 20 elements of degree 4 in 6 variables were semi-regular. I could not perform the experiment when the number of variables n was 14 since the memory of my computer was exhausted.

$n\backslash d$	2	3	4	5	6	7	8	9	10
4	.5	1	1						
5	.9	0	1	1					
6	.45	1	.45	1	1				
7		0	1	0	1	1			
8		1	.25	1	.25	1	1		
9		0	1	.65	1	0	1	1	
10			.5	1	0	1	.5	1	1
11			1	0	1	0	1	0	1
12			0.3	1	0.4	1	0.15	1	0.5
13				0	1	0.4	1	0.35	1

Table 4.2: Proportion of Samples of 20 Homogeneous Elements of Degree d in n variables that are Semi-Regular

Note that the ones on the upper two diagonals reflect that fact that all elements of degree $n-1$ or n are semi-regular, whereas the ones on the other diagonals reflect only a high probability of semi-regularity since a monomial of degree less than $n-1$ is never semi-regular. In Section 4.2.3 we show that if $d = 2^t$ and $n = 3d$ then $\sigma_{n,d}$ is semi-regular, thus establishing that the bound $d \leq n/3$ is sharp for infinitely many n.

4.2.2 Some properties of semi-regular elements

In this section we present some properties of semi-regular elements. We give a complete description of the Hilbert Series and the index of a semi-regular element. Also, we present some material that we will use in Section 4.2.3 where we present a complete characterization of the semi-regularity of the elementary symmetric polynomial.

First, we will give a complete description of the truncated series

$$\left[\frac{(1+z)^n}{1+z^d}\right]$$

when $n \leq 3d$. First, note that

$$\frac{(1+z)^n}{1+z^d} = (1+z)^n(1-z^d+z^{2d}+\cdots+(-1)^j z^{jd}+\cdots).$$

Therefore,

$$\frac{(1+z)^n}{1+z^d} = \sum_{k=0}^{\infty} \gamma(n,k,d) z^k \tag{4.1}$$

where

$$\gamma(n,k,d) = \sum_{j=0}^{\lfloor k/d \rfloor} (-1)^j \binom{n}{k-jd}.$$

Lemma 4.2.12. *Let n, and d be two natural numbers.*

(a) If k is a non-negative integer number such that $k < \lceil (n+d)/2 \rceil$ then

$$\binom{n}{k} - \binom{n}{k-d} > 0$$

(b) If $n+d$ is odd and $k = \lceil (n+d)/2 \rceil = (n+d+1)/2$ then

$$\binom{n}{k} - \binom{n}{k-d} + \binom{n}{0} \leq 0$$

Proof. Suppose k is a non-negative integer number such that $k < \lceil (n+d)/2 \rceil$. Note that $\lceil (n+d)/2 \rceil = (n+d)/2$ or $\lceil (n+d)/2 \rceil = (n+d+1)/2$. In any case since k is integer we have that $k < (n+d)/2$. Also note that

$$\binom{n}{k} - \binom{n}{k-d} > 0$$

if $k \leq n/2$. Now suppose that $n/2 \leq k < (n+d)/2$. Then $k-d < n-k \leq n/2$ so

$$\binom{n}{k} - \binom{n}{k-d} = \binom{n}{n-k} - \binom{n}{k-d} > 0$$

proving (a). Now let us suppose that $\lceil (n+d)/2 \rceil = (n+d+1)/2 = k$. Let us prove that

$$\binom{n}{k} - \binom{n}{k-d} + \binom{n}{0} \leq 0.$$

Since $(n+d+1)/2 = k$ then $(n+d)/2 < k$, thus $n-k < k-d$. Also, since $k = (n+d+1)/2 \leq (n+2d)/2$ then $k-d \leq n/2$. Therefore,

$$\binom{n}{k} - \binom{n}{k-d} = \binom{n}{n-k} - \binom{n}{k-d} < 0$$

so

$$\binom{n}{k} - \binom{n}{k-d} + \binom{n}{0} \leq 0.$$

□

Theorem 4.2.13. *Let n, and d be two natural numbers. If $n < 3d$ then*

$$\left[\frac{(1+z)^n}{1+z^d}\right] = \sum_{k=0}^{D-1} \left[\binom{n}{k} - \binom{n}{k-d}\right] z^k$$

where $D = \lceil (n+d)/2 \rceil$.

Proof. Since

$$\frac{(1+z)^n}{1+z^d} = \sum_{k=0}^{\infty} \gamma(n,k,d) z^k$$

we want to show that $\gamma(n,k,d) > 0$ if $k < \lceil (n+d)/2 \rceil$ and that $\gamma(n,k,d) \leq 0$ when $k = \lceil (n+d)/2 \rceil$. Since $n < 3d$ then $(n+d)/2 < 2d$, thus $\lceil (n+d)/2 \rceil \leq 2d$. Let k be a non-negative integer such that $k < \lceil (n+d)/2 \rceil \leq 2d$. By Lemma 4.2.12 we have that

$$\gamma(n,k,d) = \binom{n}{k} - \binom{n}{k-d} > 0.$$

Suppose now that $k = \lceil (n+d)/2 \rceil$. If $n+d$ is even, then $k = (n+d)/2 < (3d+d)/2 = 2d$ and $n - k = k - d$. So

$$\gamma(n,k,d) = \binom{n}{k} - \binom{n}{k-d} = \binom{n}{k} - \binom{n}{n-k} = 0.$$

If $n+d$ is odd then $k = (n+d+1)/2$ and $k \leq 2d$. Hence

$$\gamma(n,k,d) \leq \binom{n}{k} - \binom{n}{k-d} + \binom{n}{0} \leq 0$$

by Lemma 4.2.12. The result is proved. □

Lemma 4.2.14. *Let $d \geq 2$. Then*

$$\frac{(3d)!}{(2d+1)!(d+1)!} \geq 1$$

Proof. For $d = 2$ we have that

$$\frac{(3d)!}{(2d+1)!(d+1)!} = \frac{6!}{5!3!} = 1$$

Suppose the result is true for d let us prove it for $d+1$. By induction we have that

$$\begin{aligned}\frac{(3(d+1))!}{(2(d+1)+1)!(d+2)!} &= \frac{(3d)!}{(2d+1)!(d+1)!}\frac{(3d+1)(3d+2)(3d+3)}{(2d+2)(2d+3)(d+2)} \\ &\geq \frac{(3d+1)(3d+2)(3d+3)}{(2d+2)(2d+3)(d+2)}\end{aligned}$$

To show that

$$\frac{(3d+1)(3d+2)(3d+3)}{(2d+2)(2d+3)(d+2)} \geq 1$$

is equivalent to show that

$$23d^3 + 36d^2 + 7d - 6 \geq 0.$$

The last inequality is true since for $d \geq 2$ we have that $23d^3 + 36d^2 + 7d \geq 6$. □

Lemma 4.2.15. *Let $d \geq 2$. Then*

$$\binom{3d}{2d+1} - \binom{3d}{d+1} + \binom{3d}{1} < 0$$

Proof. Since $d \geq 2$, by above lemma we have

$$\begin{aligned}\binom{3d}{2d+1} - \binom{3d}{d+1} + \binom{3d}{1} &= \frac{(3d)!}{(2d+1)!(d-1)!} - \frac{(3d)!}{(d+1)!(2d-1)!} + 3d \\ &= \frac{(3d)!(d(d+1))}{(2d+1)!(d+1)!} - \frac{(3d)!(2d(2d+1))}{(d+1)!(2d+1)!} + 3d \\ &= \frac{(3d)!}{(2d+1)!(d+1)!}(-3d^2 - d) + 3d \\ &\leq -3d^2 - d + 3d \\ &= -3d^2 + 2d \\ &= d(-3d+2) < 0\end{aligned}$$

□

Theorem 4.2.16. *Let n, and d be two natural numbers. If $n = 3d$ and $d \geq 2$ then*

$$\left[\frac{(1+z)^n}{1+z^d}\right] = \sum_{k=0}^{2d-1} \left[\binom{n}{k} - \binom{n}{k-d}\right] z^k + z^{2d}$$

Proof. We know that

$$\frac{(1+z)^n}{1+z^d} = \sum_{k=0}^{\infty} \gamma(n,k,d) z^k.$$

Suppose $n = 3d$. Then for $k < 2d$,

$$\gamma(n,k,d) = \binom{3d}{k} - \binom{3d}{k-d} > 0$$

by Lemma 4.2.12. Also

$$\gamma(n,2d,d) = \binom{3d}{2d} - \binom{3d}{d} + \binom{3d}{0} = 1$$

and by Lemma 4.2.15

$$c_{2d+1} = \binom{3d}{2d+1} - \binom{3d}{d+1} + \binom{3d}{1} < 0.$$

This proves the result. □

Theorem 4.2.17. *Suppose that λ is a semi-regular homogeneous element of degree $d > 1$. Then $n \leq 3d$ and*

$$\mathrm{Ind}(\lambda) = \begin{cases} \lceil (n+d)/2 \rceil & \text{if } n < 3d \\ (n+d+2)/2 = 2d+1 & \text{if } n = 3d \end{cases}$$

Proof. If λ is semi-regular, then by Theorem 3.2.6

$$\mathrm{HS}_{(\lambda)}(z) = \left[\frac{(1+z)^n}{1+z^d}\right]$$

thus $\mathrm{Ind}(\lambda) = \mathrm{Ind}(1+z)^n/(1+z^d)$ so the result follows from Theorem 4.2.13 and Theorem 4.2.16. □

To finish this section, we present a theorem that will be used in the following section where we prove some results about semi-regularity of the elementary symmetric polynomials.

Lemma 4.2.18. *Let $\lambda \in B^{(n)}$ be a homogeneous element of degree d. Suppose that for $k < n$ the map*

$$B_k^{(n)} \xrightarrow{\lambda} B_{k+d}^{(n)}$$

multiplication by λ, is injective. Then the map

$$B_{k-1}^{(n)} \xrightarrow{\lambda} B_{k-1+d}^{(n)}$$

is injective.

Proof. Suppose that for $k < n$ the map

$$B_k^{(n)} \xrightarrow{\lambda} B_{k+d}^{(n)}$$

is injective. Suppose that there exists $\alpha \in B_{k-1}^{(n)}$, $\alpha \neq 0$ such that $\alpha\lambda = 0$. Since $k < n$ we have that there exits x_i such that $x_i \nmid \alpha$. So $x_i\alpha \neq 0$ and $x_i\alpha \in B_k^{(n)}$ satisfies that $x_i\alpha\lambda = 0$, which is a contradiction. □

Lemma 4.2.19. *Let k be an integer with $k \leq n$. Consider the linear form $\eta : B_n^{(n)} \to \mathbb{F}_2$ with $\eta(\alpha x_1 \cdots x_n) = \alpha$. Then $B_k^{(n)} \cong (B_{n-k}^{(n)})^*$ via the homomorphism*

$$\phi : B_k^{(n)} \to (B_{n-k}^{(n)})^*$$

where for $a \in B_k^{(n)}$ we have that $\phi(a) : B_{n-k}^{(n)} \to \mathbb{F}_2$ is the homomorphism given by $\phi(a)(b) = \eta(ab)$.

Proof. It is straightforward to see that ϕ is a linear map. Let us see that

$$\phi : B_k^{(n)} \to (B_{n-k}^{(n)})^*$$

is injective. Consider a_1, a_2 in $B_k^{(n)}$ such that $a_1 \neq a_2$. Without less of generality, let us suppose that there exists $\mu = x_{i_1} \cdots x_{i_k} \in \mathrm{Supp}(a_1) \setminus \mathrm{Supp}(a_2)$. Consider $\mu' = x_1 \cdots \hat{x}_{i_1} \cdots \hat{x}_{i_k} \cdots x_n \in B_{n-k}^{(n)}$. Thus, $\phi(a_1)(\mu') = \eta(a_1\mu') = 1$ and $\phi(a_2)(\mu') = \eta(a_2\mu') = 0$.

Therefore, $\phi(a_1) \neq \phi(a_2)$. It shows that ϕ is injective. Since $\dim B_k^{(n)} = \dim B_{n-k}^{(n)} = \dim(B_{n-k}^{(n)})^*$ then ϕ is an isomorphism. □

Lemma 4.2.20. *Let s, d, and n be natural numbers. Let $\lambda \in B^{(n)}$ be a homogeneous polynomial of degree d. Then the map*

$$B_s^{(n)} \xrightarrow{\lambda} B_{s+d}^{(n)}$$

has maximal rank if and only if the map

$$B_{n-s-d}^{(n)} \xrightarrow{\lambda} B_{n-s}^{(n)}$$

has maximal rank.

Proof. Consider the following diagram

$$\begin{array}{ccc} B_s^{(n)} & \xrightarrow{\quad\lambda\quad} & B_{s+d}^{(n)} \\ \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi_2} \\ (B_{n-s}^{(n)})^* & \xrightarrow{\lambda^*} & (B_{n-s-d}^{(n)})^* \end{array}$$

where the horizontal map λ^* is the dual map of the map multiplication by λ and the vertical maps ϕ_1, ϕ_2 are the isomophisms described in Lemma 4.2.19. Let us see that the above diagram commutes. Let $a \in B_s^{(n)}$ and $b \in B_{n-s-d}^{(n)}$. We have that

$$\phi_2(\lambda(a))(b) = \phi_2(\lambda a)(b) = \eta(\lambda a b)$$

and

$$\lambda^*(\phi_1(a))(b) = (\phi_1(a) \circ \lambda)(b) = \phi_1(a)(\lambda b) = \eta(a\lambda b)$$

It shows that the diagram commutes. Therefore, the map

$$B_s^{(n)} \xrightarrow{\lambda} B_{s+d}^{(n)}$$

has maximal rank if and only if the map

$$(B_{n-s}^{(n)})^* \xrightarrow{\lambda^*} (B_{n-s-d}^{(n)})^*$$

has maximal rank. By linear algebra we know that the map

$$(B^{(n)}_{n-s})^* \xrightarrow{\lambda^*} (B^{(n)}_{n-s-d})^*$$

has maximal rank if and only if the map

$$B^{(n)}_{n-s-d} \xrightarrow{\lambda} B^{(n)}_{n-s}$$

has maximal rank. This proves the result. □

Lemma 4.2.21. *Let $\lambda \in B^{(n)}$ be a homogeneous element of degree $d \geq 2$. Suppose $n < 3d$. Let $D = \lceil (n+d)/2 \rceil$. Suppose the map*

$$B^{(n)}_{D-d} \xrightarrow{\lambda} B^{(n)}_{D}$$

is surjective. Then, the map

$$B^{(n)}_{k-d} \xrightarrow{\lambda} B^{(n)}_{k}$$

is injective, for all $k < D$.

Proof. Suppose $n < 3d$ and consider $D = \lceil (n+d)/2 \rceil$. Suppose that the map

$$B^{(n)}_{D-d} \xrightarrow{\lambda} B^{(n)}_{D}$$

is surjective. If $n - d = 2s$ then $D = s + d$. Thus,

$$\dim B^{(n)}_{D-d} = \binom{n}{D-d} = \binom{n}{s} = \binom{n}{n-s} = \binom{n}{s+d} = \dim B^{(n)}_{D}$$

Therefore the map

$$B^{(n)}_{D-d} \xrightarrow{\lambda} B^{(n)}_{D}$$

is also injective. By Lemma 4.2.18 we have that the map

$$B^{(n)}_{k-d} \xrightarrow{\lambda} B^{(n)}_{k}$$

is injective, for all $k < D$. If $n - d = 2s + 1$ then $D = s + d + 1$. Thus,

$$\dim B^{(n)}_{D-d} = \binom{n}{D-d} = \binom{n}{s+1} = \binom{n}{n-s-1} = \binom{n}{d+s} = \dim B^{(n)}_{D-1}$$

and

$$\dim B^{(n)}_{D-d-1} = \binom{n}{D-d-1} = \binom{n}{s} = \binom{n}{n-s} = \binom{n}{s+d+1} = \dim B^{(n)}_{D}$$

Since the map

$$B^{(n)}_{D-d} \xrightarrow{\lambda} B^{(n)}_{D}$$

is surjective, by Lemma 4.2.20 we have that the map

$$B^{(n)}_{D-d-1} \xrightarrow{\lambda} B^{(n)}_{D-1}$$

is injective. Therefore, by Lemma 4.2.18 we have that

$$B^{(n)}_{k-d} \xrightarrow{\lambda} B^{(n)}_{k}$$

is injective, for all $k < D$. □

Theorem 4.2.22. *Let $\lambda \in B^{(n)}$ be a homogeneous element of degree $d \geq 2$. Suppose $n \leq 3d$.*

(a) If $n < 3d$ then λ is semi-regular if and only if for $D = \lceil (n+d)/2 \rceil$ the map

$$B^{(n)}_{D-d} \xrightarrow{\lambda} B^{(n)}_{D}$$

is surjective.

(b) If $n = 3d$ then λ is semi-regular if and only if the map

$$\frac{B^{(n)}_{d}}{\lambda B^{(n)}_{0}} \xrightarrow{\lambda} B^{(n)}_{2d}$$

is injective and the map

$$B^{(n)}_{d+1} \xrightarrow{\lambda} B^{(n)}_{2d+1}$$

is surjective.

Proof. Suppose $n < 3d$ and consider $D = \lceil (n+d)/2 \rceil$. Let us prove (a). Suppose λ is semi-regular. Then, by Theorem 4.2.17 we have that the map

$$B_{D-d}^{(n)} \xrightarrow{\lambda} B_D^{(n)}$$

is surjective. Conversely, suppose now that the map

$$B_{D-d}^{(n)} \xrightarrow{\lambda} B_D^{(n)}$$

is surjective. By Lemma 4.2.21 we have that the map

$$B_{k-d}^{(n)} \xrightarrow{\lambda} B_k^{(n)}$$

is injective, for all $k < D$. Thus, by Lemma 4.2.12 we have that for all $k < D$

$$\begin{aligned} 0 < \binom{n}{k} - \binom{n}{k-d} &= \dim(B_k^{(n)}) - \dim(B_{k-d}^{(n)}) \\ &= \dim(B_k^{(n)}) - \dim(\lambda B_{k-d}^{(n)}) \\ &= \dim\left(B_k^{(n)}/\lambda B_{k-d}^{(n)}\right). \end{aligned}$$

Therefore,

$$\begin{aligned} \mathrm{HS}_{(\lambda)}(z) &= \sum_{k=0}^{\infty} \dim\left(B_k^{(n)}/\lambda B_{k-d}^{(n)}\right) z^k \\ &= \sum_{k=0}^{D-1} \left[\binom{n}{k} - \binom{n}{k-d}\right] z^k. \end{aligned}$$

By Theorem 4.2.13

$$\left[\frac{(1+z)^n}{1+z^d}\right] = \sum_{k=0}^{D-1} \left[\binom{n}{k} - \binom{n}{k-d}\right] z^k$$

Thus,

$$\mathrm{HS}_{(\lambda)}(z) = \left[\frac{(1+z)^n}{1+z^d}\right]$$

So λ is semi-regular. This proves (a).

Let us prove (b). Suppose $n = 3d$. Suppose λ is semi-regular. By Theorem 4.2.17 we have that $\operatorname{Ind}(\lambda) = 2d + 1$. Therefore, the map

$$B_{d+1}^{(n)} \xrightarrow{\lambda} B_{2d+1}^{(n)}$$

is surjective. Since λ is semi-regular, then the map

$$\frac{B_d^{(n)}}{\lambda B_0^{(n)}} \xrightarrow{\lambda} B_{2d}^{(n)}$$

is injective. Conversely, suppose that the map

$$\frac{B_d^{(n)}}{\lambda B_0^{(n)}} \xrightarrow{\lambda} B_{2d}^{(n)}$$

is injective and the map

$$B_{d+1}^{(n)} \xrightarrow{\lambda} B_{2d+1}^{(n)}$$

is surjective. Notice that,

$$\dim B_{d-1}^{(n)} = \binom{n}{d-1} = \binom{n}{n-d+1} = \binom{3d}{2d+1} = \binom{n}{2d+1} = \dim B_{2d+1}^{(n)}$$

and

$$\dim B_{d+1}^{(n)} = \binom{n}{d+1} = \binom{n}{n-d-1} = \binom{3d}{2d-1} = \binom{n}{2d-1} = \dim B_{2d-1}^{(n)}$$

Since the map

$$B_{d+1}^{(n)} \xrightarrow{\lambda} B_{2d+1}^{(n)}$$

is surjective, then by Lemma 4.2.20 we have that the map

$$B_{d-1}^{(n)} \xrightarrow{\lambda} B_{2d-1}^{(n)}$$

is injective. Therefore, by Lemma 4.2.18 we have that

$$B_{k-d}^{(n)} \xrightarrow{\lambda} B_k^{(n)}$$

is injective, for all $k < 2d$. Thus, by Lemma 4.2.12 we have that for all $k < 2d$

$$\begin{aligned} 0 < \binom{n}{k} - \binom{n}{k-d} &= \dim(B_k^{(n)}) - \dim(B_{k-d}^{(n)}) \\ &= \dim(B_k^{(n)}) - \dim(\lambda B_{k-d}^{(n)}) \\ &= \dim\left(B_k^{(n)}/\lambda B_{k-d}^{(n)}\right). \end{aligned}$$

Since the map

$$\frac{B_d^{(n)}}{\lambda B_0^{(n)}} \xrightarrow{\lambda} B_{2d}^{(n)}$$

is injective and $\dim(B_{2d}^{(n)}) = \dim(B_d^{(n)})$ then $\dim(B_{2d}^{(n)}/\lambda B_d^{(n)}) = 1$. Putting together this information we have that

$$\begin{aligned} \mathrm{HS}_{(\lambda)}(z) &= \sum_{k=0}^{\infty} \dim\left(B_k^{(n)}/\lambda B_{k-d}^{(n)}\right) z^k \\ &= \sum_{k=0}^{2d-1} \left[\binom{n}{k} - \binom{n}{k-d}\right] z^k + z^{2d}. \end{aligned}$$

By Theorem 4.2.16

$$\left[\frac{(1+z)^n}{1+z^d}\right] = \sum_{k=0}^{2d-1} \left[\binom{n}{k} - \binom{n}{k-d}\right] z^k + z^{2d}$$

Thus,

$$\mathrm{HS}_{(\lambda)}(z) = \left[\frac{(1+z)^n}{1+z^d}\right]$$

So λ is semi-regular. This proves (b). □

4.2.3 Semi-regularity of elementary symmetric polynomials

Consider the ring of polynomials over $\mathbb{F}_2$ in n variables, $\mathbb{F}_2[X_1, ..., X_n]$. In this ring we have the elementary symmetric polynomial of degree d which is defined as

$$\sigma_d(X_1, ..., X_n) = \sum_{1 \le i_1 < \cdots < i_d \le n} X_{i_1} \cdots X_{i_d}.$$

We can consider the elementary symmetric polynomial of degree d in $B^{(n)}$, $\sigma_d(x_1, ..., x_n)$, as the image of the symmetric polynomial $\sigma_d(X_1, ..., X_n)$ under the evaluation map

$$\mathbb{F}_2[X_1, ..., X_n] \to B^{(n)}$$

$$X_i \mapsto x_i$$

To simplify we will denote $\sigma_d(x_1, ..., x_n)$ by $\sigma_{d,n}$.

In this section we give a complete description of the semi-regularity of the elementary symmetric polynomials $\sigma_{d,n}$. First, recall the following well-known identity.

Lemma 4.2.23. *Let n, d, and k be natural numbers such that $1 \leq k \leq n$ then*

$$\sigma_d(x_1, ..., x_n) = \sum_{i=0}^{d} \sigma_{d-i}(x_1, ..., x_k)\sigma_i(x_{k+1}, ..., x_n) \tag{4.2}$$

Proof. Note that

$$\begin{aligned}
\sum_{j=1}^{n} \sigma_j(x_1, ..., x_n)t^j &= \prod_{i=1}^{n}(1 + tx_i) \\
&= \prod_{i=1}^{k}(1 + tx_i) \prod_{j=1}^{n-k}(1 + tx_{j+k}) \\
&= \sum_{i=1}^{k} \sigma_i(x_1, ..., x_k)t^i \sum_{j=1}^{n-k} \sigma_j(x_{k+1}, ..., x_n)t^j
\end{aligned}$$

□

Lemma 4.2.24.

$$\sigma_{a,n}\sigma_{b,n} = \overline{\binom{a+b}{a}}\sigma_{a+b,n}$$

where $\overline{k}$ denotes the image of k in $\mathbb{F}_2$.

Proof. Let M be a monomial in $x_1, \ldots, x_n$ of degree $a+b$. Then M will occur once in $\sigma_{a,n}\sigma_{b,n}$ for each occurrence of a sub-monomial of M of degree a in $\sigma_{a,n}$. There are precisely $\binom{a+b}{a}$ such sub-monomials. □

Corollary 4.2.25.

$$\sigma_{1,n}\sigma_{k,n} = \begin{cases} 0 & \text{if } k \text{ is odd} \\ \sigma_{1+k,n} & \text{if } k \text{ is even} \end{cases}$$

Theorem 4.2.26. *Let n and k be non-negative integers. Then*

$$\overline{\binom{n}{k}} = \begin{cases} 0 & \text{if } n \text{ is even and } k \text{ is odd} \\ \overline{\binom{\lfloor n/2 \rfloor}{\lfloor k/2 \rfloor}} & \text{otherwise} \end{cases}$$

where $\overline{a}$ denotes the image of a in $\mathbb{F}_2$.

Proof. See Theorem 4.1.10 in [23]. □

Lemma 4.2.27. *Let n and l be two natural numbers. Then for all $1 \leq k \leq 2^n - 1$ we have that*

$$\overline{\binom{2^n l + j}{k}} = \begin{cases} 1 & \text{if } j = k \\ 0 & \text{if } 0 \leq j \leq k-1 \end{cases}$$

where $\overline{a}$ denotes the image of a in $\mathbb{F}_2$.

Proof. If $n = 1$, then $k = 1$ and clearly we have that $\overline{\binom{2l+1}{1}} = 1$ and $\overline{\binom{2l}{1}} = 0$. Suppose by induction that the result is true for n, let us prove it for $n+1$. For $k = 1$ we have that $\overline{\binom{2^{n+1}l+1}{1}} = 1$ and $\overline{\binom{2^{n+1}l}{1}} = 0$. Suppose $2 \leq k \leq 2^{n+1} - 1$ and $0 \leq j \leq k-1$, then $1 \leq \lfloor k/2 \rfloor \leq 2^n - 1$, and $0 \leq \lfloor j/2 \rfloor \leq \lfloor k/2 \rfloor - 1$. Suppose first that k is even. Then by Theorem 4.2.26 and by induction we have that

$$\overline{\binom{2^{n+1}l + j}{k}} = \overline{\binom{2^n l + \lfloor j/2 \rfloor}{\lfloor k/2 \rfloor}} = \begin{cases} 1 & \text{if } j = k \\ 0 & \text{if } 0 \leq j \leq k-1 \end{cases}$$

Suppose now that k is odd. Note that $2^{n+1}l + k$ is odd then by Theorem 4.2.26 and by induction we have that

$$\overline{\binom{2^{n+1}l + k}{k}} = \overline{\binom{2^n l + \lfloor k/2 \rfloor}{\lfloor k/2 \rfloor}} = 1.$$

Now if $0 \leq j \leq k-1$ is even then by Theorem 4.2.26 we have that

$$\overline{\binom{2^{n+1}l+j}{k}} = 0.$$

If $0 \leq j \leq k-1$ is odd then by Theorem 4.2.26 and induction we have that

$$\overline{\binom{2^{n+1}l+j}{k}} = \overline{\binom{2^{n}l+\lfloor j/2 \rfloor}{\lfloor k/2 \rfloor}} = 0.$$

□

Lemma 4.2.28. *The map*

$$B^{(n)}_{k-d} \xrightarrow{\sigma_{d,n}} B^{(n)}_{k}$$

is surjective if and only if there exits $\alpha \in B^{(n)}_{k-d}$ *such that* $\alpha\sigma_{d,n} = x_1 \cdots x_k$

Proof. One way is trivial. In the other way suppose that there exits $\alpha \in B^{(n)}_{k-d}$ such that $\alpha\sigma_{d,n} = x_1 \cdots x_k$. Note that the set $W := \{x_{i_1} \cdots x_{i_k} \mid 1 \leq i_1 < \cdots < i_k \leq n\}$ is a basis for the vector space $B^{(n)}_{k}$. By the natural action of the group of permutations of n-elements Σ_n on $B^{(n)}$, given $g \in \Sigma_n$ we have that

$$\begin{aligned} x_{g(1)} \cdots x_{g(k)} &= g * (x_1 \cdots x_k) \\ &= g * (\alpha\sigma_{d,n}) \\ &= (g * \alpha)(g * \sigma_{d,n}) \\ &= (g * \alpha)\sigma_{d,n} \end{aligned}$$

Therefore, for any element β in W there exits $\alpha \in B^{(n)}_{k-d}$ such that $\beta = \alpha\sigma_{d,n}$. Since W is a basis for the vector space $B^{(n)}_{k}$, and the map

$$B^{(n)}_{k-d} \xrightarrow{\sigma_{d,n}} B^{(n)}_{k}$$

is a homomorphism then the map is a surjective. □

The next theorem is one of the key results of this section.

Theorem 4.2.29. *Let $d = 2^m l$. Then $\sigma_{d,n}$ is semi-regular for all $n = d + i$, with $0 \leq i \leq 2^{m+1} - 1$.*

Proof. For $0 \leq i \leq 1$ the result follows from Theorem 4.2.2. Now notice that for all $n = d+i$ with $0 \leq i \leq 2^{m+1} - 1$ we have that $n < 3d$. Thus, by Theorem 4.2.22 we need to prove that for $D = \lceil (n + d)/2 \rceil$ the map

$$B_{D-d}^{(n)} \xrightarrow{\sigma_{d,n}} B_D^{(n)}$$

is surjective. Let us suppose that $i \geq 2$ is an even number. Thus, $2 \leq i \leq 2^{m+1} - 2$. Taking $k = i/2$ we have that $1 \leq k \leq 2^m - 1$, $n = d + i = d + 2k$ and

$$D = \left\lceil \frac{d + i + d}{2} \right\rceil = d + k.$$

Since $D = d + k$, we need to show that

$$B_k^{(n)} \xrightarrow{\sigma_{d,n}} B_{d+k}^{(n)}$$

is surjective. By Lemma 4.2.23 and Lemma 4.2.24 we have that

$$\begin{aligned}
\sigma_{k,d+k}\sigma_{d,n} &= \sigma_{k,d+k}\sigma_{d,d+2k} \\
&= \sigma_{k,d+k} \sum_{j=0}^{d} \sigma_{d-j,d+k}\sigma_j(x_{d+k+1}, ..., x_{d+2k}) \\
&= \sum_{j=0}^{d} \overline{\binom{d+k-j}{k}} \sigma_{d+k-j,d+k}\sigma_j(x_{d+k+1}, ..., x_{d+2k}).
\end{aligned}$$

Since $1 \leq k \leq 2^m - 1$ by Lemma 4.2.27 we have that

$$\overline{\binom{d+k-j}{k}} = 0$$

for all $1 \leq j \leq d$, and

$$\overline{\binom{d+k}{k}} = 1$$

Therefore,

$$\sigma_{k,d+k}\sigma_{d,n} = \sigma_{d+k,d+k} = x_1 \cdots x_{d+k}.$$

By Lemma 4.2.28 the map is onto. Suppose now that $i \geq 2$ is odd. Thus, $3 \leq i \leq 2^{m+1} - 1$. Taking $k = (i+1)/2$ we have that $2 \leq k \leq 2^m$, $n = d + i = d + 2k - 1$ and

$$D = \left\lceil \frac{d + i + 1 + d}{2} \right\rceil = d + k.$$

Since $k = D - d$, we want to show that

$$B_k^{(n)} \xrightarrow{\sigma_{d,n}} B_{d+k}^{(n)}$$

is surjective. By Lemma 4.2.23 and Lemma 4.2.24 we have that

$$\begin{aligned}
\sigma_{k-1,d+k}\sigma_{d,n} &= \sigma_{k-1,d+k}\sigma_{d,d+2k-1} \\
&= \sigma_{k-1,d+k} \sum_{j=0}^{d} \sigma_{d-j,d+k}\sigma_j(x_{d+k+1}, ..., x_{d+2k-1}) \\
&= \sum_{j=0}^{d} \overline{\binom{d+k-1-j}{k-1}} \sigma_{d+k-1-j,d+k}\sigma_j(x_{d+k+1}, ..., x_{d+2k-1}).
\end{aligned}$$

Since $2 \leq k \leq 2^m$, then $1 \leq k - 1 \leq 2^m - 1$. Thus, by Lemma 4.2.27 we have that

$$\overline{\binom{d+k-1-j}{k-1}} = 0$$

for all $1 \leq j \leq d$, and

$$\overline{\binom{d+k-1}{k-1}} = 1$$

Therefore,

$$\sigma_{k-1,d+k}\sigma_{d,n} = \sigma_{d+k-1,d+k}.$$

Therefore, $x_1\sigma_{k-1,d+k} \in B_k^{(n)}$ and $x_1\sigma_{k-1,d+k}\sigma_{d,n} = x_1\sigma_{d+k-1,d+k} = \sigma_{d+k,d+k} = x_1 \cdots x_{d+k}$. By Lemma 4.2.28 the map is onto. □

Lemma 4.2.30. *Let m be a positive integer*

$$\overline{\binom{j}{2^m}} = \begin{cases} 0 & \text{if } j = 2^{m+1} \\ 1 & \text{if } 2^m \leq j \leq 2^{m+1} - 1 \end{cases}$$

where $\overline{k}$ denotes the image of k in $\mathbb{F}_2$.

Proof. If $m = 1$ we have that

$$\overline{\binom{4}{2}} = 0, \text{ and } \overline{\binom{3}{2}} = \overline{\binom{2}{2}} = 1.$$

Suppose the result is true for $m \geq 1$ let us prove that it is true for $m + 1$. Note that by Theorem 4.2.26 and induction

$$\overline{\binom{2^{m+2}}{2^{m+1}}} = \overline{\binom{2^{m+1}}{2^m}} = 0.$$

Now, if $2^{m+1} \leq j \leq 2^{m+2} - 1$, then $2^m \leq \lfloor j/2 \rfloor \leq 2^{m+1} - 1$ so by Theorem 4.2.26 and induction

$$\overline{\binom{j}{2^{m+1}}} = \overline{\binom{\lfloor j/2 \rfloor}{2^m}} = 1.$$

□

Lemma 4.2.31. *Let $d = 2^m$ and $n = 3d = 2^{m+1} + 2^m$. Then*

$$\sigma_d(x_{i_1}, \ldots, x_{i_{2^{m+1}}})\sigma_{d,n} = x_{i_1} \cdots x_{i_{2^{m+1}}} + \sigma_{2d,n}$$

Proof. Let $\mu \in \text{Supp}(\sigma_{2d,n})$. Let j be the number of common variables between μ and $x_{i_1} \cdots x_{i_{2^{m+1}}}$. Note that $2^m \leq j \leq 2^{m+1}$. μ will occur once in the product $\sigma_d(x_{i_1}, \ldots, x_{i_{2^{m+1}}})\sigma_{d,n}$ for each occurrence of a sub-monomial of μ of degree $d = 2^m$ in $\sigma_d(x_{i_1}, \ldots, x_{i_{2^{m+1}}})$. There are exactly $\binom{j}{2^m}$ such sub-monomials. If $j = 2^{m+1}$ then $\mu = x_{i_1} \cdots x_{i_{2^{m+1}}}$ and by the above lemma this element appears an even number of times. So

$x_{i_1}\cdots x_{i_{2^{m+1}}} \notin \mathrm{Supp}(\sigma_d(x_{i_1},\ldots,x_{i_{2^{m+1}}})\sigma_{d,n})$. If $2^m \leq j \leq 2^{m+1}-1$ then by above lemma this element appears an odd number of times. So $\mu \in \mathrm{Supp}(\sigma_d(x_{i_1},\ldots,x_{i_{2^{m+1}}})\sigma_{d,n})$. Thus,

$$\sigma_d(x_{i_1},\ldots,x_{i_{2^{m+1}}})\sigma_{d,n} = x_{i_1}\cdots x_{i_{2^{m+1}}} + \sigma_{2d,n}.$$

□

Lemma 4.2.32. *Let $d = 2^m$ and $n = 3d$. Then the map*

$$B_{d+1}^{(n)} \xrightarrow{\sigma_d} B_{2d+1}^{(n)}$$

is surjective.

Proof. First, let us see that

$$\sigma_{d-1,2d+1}\sigma_{d,n} = \sigma_{2d-1,2d+1}.$$

By Lemma 4.2.23, Lemma 4.2.24 and Lemma 4.2.27 we have

$$\begin{aligned}
\sigma_{d-1,2d+1}\sigma_{d,n} &= \sigma_{k,d+k}\sum_{j=0}^{d}\sigma_{d-j,2d+1}\sigma_j(x_{2d+2},...,x_{3d}) \\
&= \sum_{j=0}^{d}\overline{\binom{d+(d-1-j)}{d-1}}\sigma_{2d-1-j,2d+1}\sigma_j(x_{2d+2},...,x_{3d}) \\
&= \sum_{j=0}^{d}\overline{\binom{2^m+(2^m-1-j)}{2^m-1}}\sigma_{2d-1-j,2d+1}\sigma_j(x_{2d+2},...,x_{3d}) \\
&= \sigma_{2d-1,2d+1}.
\end{aligned}$$

Note that

$$\begin{aligned}
\sigma_{2d-1,2d+1} &= x_1\sigma_{2d-2}(x_2,...,x_{2d+1}) + x_2\sigma_{2d-2}(x_1,x_3,...,x_{2d-2}) \\
&\quad + x_1x_2\sigma_{2d-3}(x_3,...,x_{2d-2}) + x_3\cdots x_{2d+1}.
\end{aligned}$$

Therefore

$$x_1x_2\sigma_{d-1,2d+1}\sigma_{d,n} = x_1x_2\sigma_{2d-1,2d+1} = x_1x_2x_3\cdots x_{2d+1}.$$

Since $x_1x_2\sigma_{d-1,2d+1} \in B_{d+1}^{(n)}$ then by Lemma 4.2.28 the map is onto. □

Theorem 4.2.33. *Let $d = 2^m$. If $n = d + 2^{m+1}$ then $\sigma_{d,n}$ is semi-regular.*

Proof. Suppose $n = d + 2^{m+1}$ then $n = 3d$. By Theorem 4.2.22 we want to show that the map

$$\frac{B_d^{(n)}}{\sigma_{d,n}B_0^{(n)}} \xrightarrow{\sigma_{d,n}} B_{2d}^{(n)}$$

is injective and the map

$$B_{d+1}^{(n)} \xrightarrow{\sigma_{d,n}} B_{2d+1}^{(n)}$$

is surjective. By Lemma 4.2.32 the map

$$B_{d+1}^{(n)} \xrightarrow{\sigma_{d,n}} B_{2d+1}^{(n)}$$

is surjective. Now, by Lemma 4.2.31 we have that

$$\sigma_d(x_{i_1}, \ldots, x_{i_{2d}})\sigma_{d,n} = x_{i_1} \cdots x_{i_{2d}} + \sigma_{2d,n}.$$

Consider the set

$$S = \{x_{i_1} \cdots x_{i_{2d}} + \sigma_{2d,n} \mid 1 \leq i_1 \leq \cdots \leq i_{2d} \leq n\}$$

Note that the set $S \setminus \{x_1 \cdots x_{2^{m+1}} + \sigma_{2d,n}\} \subset B_{2d}^{(n)}$ is linearly independent. And this set has $\binom{n}{2d} - 1 = \dim B_{2d}^{(n)} - 1$ elements. Therefore the map

$$\frac{B_d^{(n)}}{\sigma_d B_0^{(n)}} \xrightarrow{\sigma_{d,n}} B_{2d}^{(n)}$$

is injective. By all the above, $\sigma_{d,n}$ is semi-regular. □

The following theorem is our main result of this section.

Theorem 4.2.34. *Let $d \geq 2$, where $d = 2^m l$ with l an odd number, and m a non-negative integer. Then*

(a) If $l > 1$, $\sigma_{d,n}$ is semi-regular if and only if $n = d, d+1, ..., d + 2^{m+1} - 1$.

(b) If $l = 1$, $\sigma_{d,n}$ is semi-regular if and only if $n = d, d+1, ..., d+2^{m+1}$.

Proof. Suppose that $\sigma_{d,n}$ is semi-regular. Let us suppose first that $l = 1$. Therefore, $d = 2^m$, with $m \geq 1$. By Theorem 4.2.10 we have that $n \leq 3d = 2^m(1+2) = 2^m + 2^{m+1} = d + 2^{m+1}$. By Theorem 4.2.29 and Theorem 4.2.33 we have that $\sigma_{d,n}$ is semi-regular for $n = d, d+1, ..., d+2^{m+1}$. So (b) is proved. Suppose now that $l > 1$. By Corollary 4.2.17

$$\mathrm{Ind}(\sigma_{d,n}) \geq \left\lceil \frac{n+d}{2} \right\rceil \geq \frac{n+d}{2}.$$

Note that

$$\sigma_{2^m,n}\sigma_{d,n} = \overline{\binom{2^m l + 2^m}{2^m}}\sigma_{2^m+d,n} = \overline{\binom{l+1}{1}}\sigma_{2^m+d,n} = 0.$$

Since $l > 1$, then $2^m < 2^m l = d$. So, we have that $\sigma_{2^m,n} \notin (\sigma_{d,n})$. Thus $\mathrm{D_{ff}}(\sigma_{d,n}) \leq d + 2^m$. Since $\sigma_{d,n}$ is semi-regular we have that $\mathrm{Ind}(\sigma_{d,n}) \leq \mathrm{D_{ff}}(\sigma_{d,n})$. So $n + d \leq 2d + 2^{m+1}$ from which we obtain $n \leq d + 2^{m+1}$. Suppose $n = d + 2^{m+1} = 2^{m+1}l + 2^{m+1}$. Since $l > 1$ then $n < 3d$. Thus, if $\sigma_{d,n}$ is semi-regular then $\mathrm{Ind}(\sigma_{d,n}) = \lceil (n+d)/2 \rceil = d + 2^m$. By Theorem 4.2.22 the map

$$B_{2^m}^{(n)} \xrightarrow{\sigma_{d,n}} B_{d+2^m}^{(n)}$$

is surjective. However,

$$\begin{aligned} \dim B_{2^m}^{(n)} = \binom{n}{2^m} &= \binom{d+2^{m+1}}{2^m} \\ &= \binom{d+2^{m+1}}{d+2^m} \\ &= \dim B_{d+2^m}^{(n)}. \end{aligned}$$

So the map

$$B_{2^m}^{(n)} \xrightarrow{\sigma_{d,n}} B_{d+2^m}^{(n)}$$

is injective. But that is not possible since $\sigma_{2^m,n}\sigma_{d,m} = 0$. Hence we must have $n \leq d + 2^{m+1} - 1$. Conversely, by Theorem 4.2.29, $\sigma_{d,n}$ is semi-regular for $n = d, d+1, ..., d+2^{m+1}-1$. It proves (a). □

The following table gives a visual interpretation of Theorem 4.2.34.

$n\backslash d$	2	3	4	5	6	7	8	9	10	11	12	13	14
2	x												
3	x	x											
4	x	x	x										
5	x		x	x									
6	x		x	x	x								
7			x		x	x							
8			x		x	x	x						
9			x		x		x	x					
10			x				x	x	x				
11			x				x		x	x			
12			x				x		x	x	x		
13							x		x		x	x	
14							x				x	x	x

Table 4.3: Semi-Regularity of $\sigma_{d,n}$. The values when $\sigma_{d,n}$ is semi-regular are marked with an x

4.2.4 Semi-regularity of the sequence $X_1^2, \ldots, X_n^2, \lambda'$

Let $S^{(n)} = \mathbb{F}_2[X_1, ..., X_n]$ be the ring of polynomials in n-variables over the field $\mathbb{F}_2$. Let $B^{(n)} = \mathbb{F}_2[X_1, ..., X_n]/(X_1^2, ..., X_n^2)$. Denote the image of X_i in $B^{(n)}$ by x_i. Given $\lambda \in B^{(n)}$ let us denote by λ' the natural lifting of λ in $S^{(n)}$. Given $\lambda \in B^{(n)}$ a homogeneous element with $\deg(\lambda) = d$ we will give some results about semi-regularity on $S^{(n)}$ of the sequence $X_1^2, \ldots, X_n^2, \lambda'$. We know by Theorem 3.1.3 that the sequence $X_1^2, \ldots, X_n^2, \lambda'$ is semi-regular on $S^{(n)}$ if and only if

$$\mathrm{HS}_I(z) = \left[\frac{(1-z^2)^n(1-z^d)}{(1-z)^n}\right]$$

where $I = (X_1^2, \ldots, X_n^2, \lambda')$. Note that

$$\left[\frac{(1-z^2)^n(1-z^d)}{(1-z)^n}\right] = \left[(1+z)^n(1-z^d)\right]$$

Lemma 4.2.35. *Let n, d be two natural numbers.*

(a) If k is a non-negative integer number such that $k < \lceil (n+d)/2 \rceil$ then

$$\binom{n}{k} - \binom{n}{k-d} > 0$$

(b) If $k = \lceil (n+d)/2 \rceil$ *then*

$$\binom{n}{k} - \binom{n}{k-d} \leq 0$$

Proof. Part (a) is proved in Lemma 4.2.12. Now let us suppose that $k = \lceil (n+d)/2 \rceil$. We want to show that

$$\binom{n}{k} - \binom{n}{k-d} \leq 0$$

If $k = \lceil (n+d)/2 \rceil = (n+d+1)/2$ then $(n+d)/2 < k$, thus $n-k < k-d$. Also, since $k = (n+d+1)/2 \leq (n+2d)/2$ then $k - d \leq n/2$. Therefore,

$$\binom{n}{k} - \binom{n}{k-d} = \binom{n}{n-k} - \binom{n}{k-d} < 0$$

If $k = \lceil (n+d)/2 \rceil = (n+d)/2$ then $n - k = k - d$. Thus

$$\binom{n}{k} - \binom{n}{k-d} = 0$$

Therefore (b) is proved. □

Theorem 4.2.36. *Let* n, d *be two natural numbers and let* $D = \lceil (n+d)/2 \rceil$. *Then*

$$\left[(1+z)^n (1-z^d)\right] = \sum_{k=0}^{D-1} \left[\binom{n}{k} - \binom{n}{k-d} \right] z^k$$

Proof. Clearly we have

$$(1+z)^n (1-z^d) = \sum_{k=0}^{\infty} \left[\binom{n}{k} - \binom{n}{k-d} \right] z^k$$

By Lemma 4.2.35 we have that

$$\binom{n}{k} - \binom{n}{k-d} > 0$$

if $k < D$, and

$$\binom{n}{k} - \binom{n}{k-d} \leq 0$$

if $k = D$. Therefore,

$$(1+z)^n(1-z^d) = \sum_{k=0}^{\infty} \left[\binom{n}{k} - \binom{n}{k-d} \right] z^k$$

□

Theorem 4.2.37. *Let $\lambda \in B^{(n)}$ be a homogeneous element with $\deg(\lambda) = d > n/3$. Then λ is semi-regular on $B^{(n)}$ if an only if $X_1^2, \ldots, X_n^2, \lambda'$ is semi-regular on $S^{(n)}$.*

Proof. Let $\lambda \in B^{(n)}$ be a homogeneous element with $\deg(\lambda) = d > n/3$. Let $D = \lceil (n+d)/2 \rceil$. By Theorem 3.2.6 and Theorem 4.2.13 we have that λ is semi-regular on $B^{(n)}$ if and only if

$$\mathrm{HS}_{(\lambda)}(z) = \left[\frac{(1+z)^n}{1+z^d} \right] = \sum_{k=0}^{D-1} \left[\binom{n}{k} - \binom{n}{k-d} \right] z^k$$

Also by Theorem 3.1.3 and Theorem 4.2.36 we have that $X_1^2, \ldots, X_n^2, \lambda'$ is semi-regular on $S^{(n)}$ if and only if

$$\mathrm{HS}_I(z) = \left[(1+z)^n)(1-z^d) \right] = \sum_{k=0}^{D-1} \left[\binom{n}{k} - \binom{n}{k-d} \right] z^k$$

where $I = (X_1^2, \ldots, X_n^2, \lambda')$. □

Theorem 4.2.38. *Let $\hat{\lambda} \in S^{(n)}$ be a homogeneous element with $\deg(\hat{\lambda}) = d$ and $2 \leq d \leq n/3$. Then $X_1^2, \ldots, X_n^2, \hat{\lambda}$ is not a semi-regular sequence on $S^{(n)}$.*

Proof. Let $\hat{\lambda} \in S^{(n)}$ be a homogeneous element with $\deg(\hat{\lambda}) = d$ and $2 \leq d \leq n/3$. Consider $J = (X_1^2, \ldots, X_n^2, \hat{\lambda})$. Suppose that $\hat{\lambda} \in (X_1^2, \ldots, X_n^2)$. Note that $d_{reg}(J) = \min\{k \geq 0 \mid J \cap S_k = S_k\} > d$. Thus, $1\hat{\lambda} \in (X_1^2, \ldots, X_n^2)$ and $\deg 1 + \deg \hat{\lambda} = d < d_{reg}(J)$. However, $1 \notin (X_1^2, \ldots, X_n^2)$, therefore the sequence $X_1^2, ..., X_n^2, \hat{\lambda}$ cannot be semi-regular on $S^{(n)}$. Suppose now that $\hat{\lambda} \notin (X_1^2, \ldots, X_n^2)$. Consider λ as the image of the polynomial $\hat{\lambda}$ under the evaluation map

$$\mathbb{F}_2[X_1, ..., X_n] \to B^{(n)}$$

$$X_i \mapsto x_i$$

Since $\hat{\lambda} \notin (X_1^2, \ldots, X_n^2)$ then $\lambda \in B^{(n)}$ is a homogeneous element with $\deg(\lambda) = d$ and $2 \leq d \leq n/3$. Consider λ' the natural lifting of λ in $S^{(n)}$. Note that the ideals $I = (X_1^2, ..., X_n^2, \lambda')$ and $J = (X_1^2, ..., X_n^2, \hat{\lambda})$ are the same ideal in the ring $S^{(n)}$. By Theorem 3.1.3 we have that the sequence $X_1^2, ..., X_n^2, \hat{\lambda}$ is semi-regular if and only if the sequence $X_1^2, ..., X_n^2, \lambda'$ is semi-regular. Let us show that the sequence is $X_1^2, ..., X_n^2, \lambda'$ not semi-regular on $S^{(n)}$. Suppose first that $d < n/3$. By Theorem 4.2.10 we have that λ is no semi-regular on $B^{(n)}$ so by Theorem 3.3.1, $X_1^2, \ldots, X_n^2, \lambda'$ cannot be a semi-regular sequence on $S^{(n)}$. Suppose now that $d = n/3$. If $X_1^2, \ldots, X_n^2, \lambda'$ is a semi-regular sequence on $S^{(n)}$ then by Theorem 3.3.1, λ is semi-regular on $B^{(n)}$. Consider $I = (X_1^2, \ldots, X_n^2, \lambda')$. By Theorem 4.2.36, Theorem 3.1.3, Theorem 3.2.6 and Theorem 4.2.16 we have that

$$\begin{aligned}
\sum_{k=0}^{2d-1} \left[\binom{n}{k} - \binom{n}{k-d} \right] z^k &= \left[(1+z)^n)(1-z^d) \right] \\
&= \mathrm{HS}_I(z) \\
&= \mathrm{HS}_{(\lambda)}(z) \\
&= \left[\frac{(1+z)^n}{1+z^d} \right] \\
&= \sum_{k=0}^{2d-1} \left[\binom{n}{k} - \binom{n}{k-d} \right] z^k + z^{2d}
\end{aligned}$$

which is a contradiction. Therefore, $X_1^2, \ldots, X_n^2, \lambda'$ cannot be a semi-regular sequence on $S^{(n)}$. □

As we metioned in Section 4.2.1, it was observed in [26, Lemma 3.12], that the element

$$\sum_{1 \leq i < j \leq n} x_i x_j \subset B^{(n)}$$

is not semi-regular for any $n \geq 7$, contradicting what Bardet asserts in Proposition 3.2.13 in [3]. Moreover, Bardet asserts in the same proposition that the sequence

$$X_1^2, \ldots, X_n^2, \sum_{1 \leq i < j \leq n} X_i X_j \subset S^{(n)}$$

is semi-regular for all n. Theorem 4.2.38 implies that this sequence is not semi-regular for any $n > 5$.

Now we will give a complete characterization of the semi-regularity of the sequence $X_1^2, \ldots, X_n^2, \sigma'_d(X_1, \ldots, X_n)$ in the ring $S^{(n)}$, where $\sigma'_d(X_1, \ldots, X_n)$ is the elementary symmetric polynomial of degree d which is defined as

$$\sigma'_d(X_1, ..., X_n) = \sum_{1 \leq i_1 < \cdots < i_d \leq k} X_{i_1} \cdots X_{i_d}$$

Let us consider the symmetric polynomial of degree d in $B^{(n)}$, $\sigma_d(x_1, ..., x_n)$, as the image of the symmetric polynomial $\sigma'_d(X_1, ..., X_n)$ under the evaluation map

$$\mathbb{F}_2[X_1, ..., X_n] \to B^{(n)}$$

$$X_i \mapsto x_i$$

Theorem 4.2.39. *Let $2 \leq d$, where $d = 2^m l$ with l an odd number, and m a non-negative integer. The sequence $X_1^2, \ldots, X_n^2, \sigma'_{d,n}$ is semi-regular on $S^{(n)}$ if and only if $n = d, \ldots, d + 2^{m+1} - 1$.*

Proof. First suppose that $d = 2^m l$ with $l > 1$. Suppose that $X_1^2, \ldots, X_n^2, \sigma'_{d,n}$ is semi-regular on $S^{(n)}$. By Theorem 3.3.1 we have that $\sigma_{d,n}$ is semi-regular over $\mathbb{F}_2$ and by Theorem 4.2.34 we have that $d \leq n \leq d + 2^{m+1} - 1$. Conversely, suppose that $d \leq n \leq d + 2^{m+1} - 1$. By Theorem 4.2.34 we have that $\sigma_{d,n}$ is semi-regular over $\mathbb{F}_2$. Note that $n \leq d + 2^{m+1} - 1 \leq d + 2d - 1 = 3d - 1 < 3d$. Thus by Theorem 4.2.37 since $\sigma_{d,n}$ is semi-regular then the sequence $X_1^2, \ldots, X_n^2, \sigma'_{d,n}$ is semi-regular on $S^{(n)}$.

Suppose now that $d = 2^m \geq 2$. Suppose that $X_1^2, \ldots, X_n^2, \sigma'_{d,n}$ is semi-regular. By Theorem 4.2.38 we must have that $n \leq 3d-1 = d+2^{m+1}-1$. Conversely, if $n \leq d+2^{m+1}-1 < 3d$ then by Theorem 4.2.34, $\sigma_{d,n}$ is semi-regular over $\mathbb{F}_2$, so by Theorem 4.2.37 the sequence $X_1^2, \ldots, X_n^2, \sigma'_{d,n}$ is semi-regular. □

4.2.5 Index of λ, $n \leq 3d$ case

As it is mentioned at the end of Section 3.2.1, it would be interesting to know whether $\mathrm{Ind}((\lambda_1, \ldots, \lambda_m)) \geq \mathrm{Ind}(T_{\mathbf{d},n}(z))$ for an arbitrary sequence $\lambda_1, \ldots, \lambda_m$. Thus, we have the following conjecture.

Conjecture 5. Let $\lambda_1, ..., \lambda_m$ be a sequence of homogeneous elements in $B^{(n)}$ where $\deg(\lambda_i) = d_i$. Let $\mathbf{d} = (d_1, \ldots, d_m)$. Then

$$\mathrm{Ind}((\lambda_1, ..., \lambda_m)) \geq \mathrm{Ind}(T_{\mathbf{d},n}(z))$$

We can give a partial positive answer for this conjecture in the case $m = 1$.

Theorem 4.2.40. *Let $\lambda \in B^{(n)}$ be homogeneous of degree d. If $n \leq 3d$ then*

$$\mathrm{Ind}(\lambda) \geq \mathrm{Ind}(T_{(d),n}(z))$$

Proof. Let $\lambda \in B^{(n)}$ be homogeneous of degree d. Note that

$$\mathrm{HS}_{(\lambda)}(z) = \sum_{k=0}^{\infty} \dim(B_k^{(n)}/\lambda B_{k-d}^{(n)})$$

Let $n \leq 3d$, we want to show that $\mathrm{Ind}\,\mathrm{HS}_{(\lambda)}(z) = \mathrm{Ind}(\lambda) \geq \mathrm{Ind}\,T_{(d),n}(z)$. First, suppose that $n < 3d$. By Theorem 4.2.13 we have that $\mathrm{Ind}(T_{(d),n}(z)) = D$ where $D = \lceil (n+d)/2 \rceil$. Moreover

$$[T_{(d),n}(z)] = \left[\frac{(1+z)^n}{1+z^d}\right] = \sum_{k=0}^{D-1} \left[\binom{n}{k} - \binom{n}{k-d}\right] z^k$$

Therefore for all $k < D$

$$0 < \binom{n}{k} - \binom{n}{k-d} = \dim B_k^{(n)} - \dim B_{k-d}^{(n)}$$

Thus for all $k < D$ we have

$$\begin{aligned} \dim(B_k^{(n)}/\lambda B_{k-d}^{(n)}) &= \dim B_k^{(n)} - \dim \lambda B_{k-d}^{(n)} \\ &\geq \dim B_k^{(n)} - \dim B_{k-d}^{(n)} \\ &> 0 \end{aligned}$$

Therefore $\operatorname{Ind}(\lambda) = \operatorname{Ind} \mathrm{HS}_{(\lambda)}(z) \geq D = \operatorname{Ind} T_{(d),n}(z)$.

Suppose now that $n = 3d$. Let us prove that $\dim(B_k^{(n)}/\lambda B_{k-d}^{(n)}) > 0$ for all $k \leq 2d$. By Theorem 4.2.16 we have that $\operatorname{Ind}(T_{(d),n}(z)) = 2d + 1$. Moreover

$$[T_{(d),n}(z)] = \left[\frac{(1+z)^n}{1+z^d}\right] = \sum_{k=0}^{2d-1} \left[\binom{n}{k} - \binom{n}{k-d}\right] z^k + z^{2d}$$

Then for all $k < 2d$

$$0 < \binom{n}{k} - \binom{n}{k-d} = \dim B_k^{(n)} - \dim B_{k-d}^{(n)}$$

As we saw above this implies that for all $k < 2d$

$$\dim(B_k^{(n)}/\lambda B_{k-d}^{(n)}) > 0$$

Now, note that λ is in the kernel of the map

$$B_d^{(n)} \xrightarrow{\lambda} B_{2d}^{(n)}$$

Thus, dimension of the kernel is at least 1, so $\dim(\lambda B_d^{(n)}) \leq \dim(B_d^{(n)}) - 1$. Since $n = 3d$ we have that $\dim B_{2d}^{(n)} = \dim B_d^{(n)}$, therefore

$$\begin{aligned} \dim(B_{2d}^{(n)}/\lambda B_d^{(n)}) &= \dim(B_{2d}^{(n)}) - \dim(\lambda B_d^{(n)}) \\ &\geq \dim B_{2d}^{(n)} - \dim B_d^{(n)} + 1 \\ &= 1 \end{aligned}$$

Thus, $\dim(B_k^{(n)}/\lambda B_{k-d}^{(n)}) > 0$ for all $k \leq 2d$. Therefore $\operatorname{Ind}(\lambda) = \operatorname{Ind} \mathrm{HS}_{(\lambda)}(z) \geq 2d + 1 = \operatorname{Ind} T_{(d),n}(z)$. □

4.3 Most homogeneous sequences are semi-regular

In her thesis [3, §3.1] Bardet states "Nous conjecturons tout de mème qu'une suite 'tiré au hazard' sera semi-régulière sur $\mathbb{F}_2$, dans le sens ou la proportion de suites semi-régulières

tend vers 1 quand n tend vers l'infini" (We conjecture none the less that a sequence 'chosen at random' will be $\mathbb{F}_2$-semi-regular in the sense that the proportion of sequences that are semi-regular tends to 1 as n tends to infinity). Notice that this conjecture is ambiguous in the sense that it is not defined precisely the meaning of " proportion of semi-regular sequences". If the proportion of semi-regular sequences in the ring $B^{(n)}$ is interpreted as the quotient $s(n)/h(n)$ where $h(n)$ is the number of subsets of $B^{(n)}$ consisting of homogeneous elements of degree greater than or equal to one and $s(n)$ is the number of such subsets that are semi-regular then the conjecture was proved to be true by J. Schlather. He proved that

$$\lim_{n\to\infty} \frac{s(n)}{h(n)} = 1$$

In this section we will present the proof of this result.

Lemma 4.3.1. *Let k be a positive integer and suppose that $\{\lambda_1, \ldots, \lambda_m\}$ spans B_k. Then $\lambda_1, \ldots, \lambda_m$ is a semi-regular sequence.*

Proof. Notice that $\deg(\lambda_i) = k$ so $(\lambda_1, \ldots, \lambda_m) \cap B_j = \{0\}$ for all $j < k$. On the other hand, $(\lambda_1, \ldots, \lambda_m) \cap B_k = B_k$, so $\mathrm{Ind}(\lambda_1, \ldots, \lambda_m) = k$. For any homogeneous $f \in B$ we have $\deg(f) + \deg(\lambda_i) \geq k$ so k-semi-regularity is trivially satisfied. □

Lemma 4.3.2. *Let $\{\lambda_1, \ldots, \lambda_m\}$ be a semi-regular sequence of homogeneous elements of B and let $D = \mathrm{Ind}(\lambda_1, \ldots, \lambda_m)$. If $\nu \in B$ is a homogeneous element of degree greater than or equal to D then $\lambda_1, \ldots, \lambda_m, \nu$ is also semi-regular.*

Proof. Since $\deg(\nu) \geq D$ we have

$$(\lambda_1, \ldots, \lambda_m) = (\lambda_1, \ldots, \lambda_m, \nu)$$

so the degree of regularity does not change and again we see for any homogeneous $f \in B$ that $\deg(f) + \deg(\nu) \geq D$. So D-semi-regularity is again trivially verified. □

Proposition 4.3.3. *Let V_n be an n-dimensional $\mathbb{F}_2$-vector space and let $\mathcal{P}(V_n\backslash\{0\})$ be the set of subsets of $V_n\backslash\{0\}$. Let S_n be the number of subsets of $V_n\backslash\{0\}$ that span V_n. Then*

$$\lim_{n\to\infty} \frac{S_n}{|\mathcal{P}(V_n\backslash\{0\})|} = 1$$

Equivalently the probability of randomly picked subset of V_n being a spanning set goes to 1 as $n \to \infty$.

Proof. To prove the result it is enough to prove that the probability of a randomly selected subset of V_n not being a spanning set goes to 0 as $n \to \infty$. Let A be subset of V_n that does not span V_n. Since A does not span V_n then $A \subseteq V'$ where V' is a $(n-1)$-dimensional subspace of V_n. Note that $|\mathcal{P}(V_n)| = 2^{2^n}$ and $|\mathcal{P}(V')| = 2^{2^{n-1}}$. Therefore, the probability that A is contained in a particular $(n-1)$-dimensional subspace is $2^{2^{n-1}}/2^{2^n} = 1/2^{2^{n-1}}$. It is well known that the number of different m-dimensional vector subspaces of an n-dimensional vector space over a finite field $\mathbb{F}q$ is given by the Gaussian binomial coefficient

$$\binom{n}{m}_q = \frac{(q^n-1)\cdots(q^n-q^{m-1})}{(q^m-1)\cdots(q^m-q^{m-1})}$$

Therefore, the number of $(n-1)$-dimensional subspaces of V_n is

$$\binom{n}{n-1}_2 = \frac{(2^n-1)\cdots(2^n-2^{n-2})}{(2^{n-1}-1)\cdots(2^{n-1}-2^{n-2})} = 2^n - 1$$

Thus, the probability that a randomly selected subset of V_n is not a spanning set is bounded by $(2^n-1)/2^{2^{n-1}}$. Taking a limit we have

$$\lim_{n\to\infty} \frac{2^n-1}{2^{2^{n-1}}} = 0$$

This shows that the probability of a randomly selected subset of V_n not being a spanning set goes to 0 as $n \to \infty$. □

Theorem 4.3.4. *Let d and n be positive integers with $d < n$ and let $P_d(n)$ be the proportion of homogeneous sequences of degree greater than or equal to d in $B^{(n)}$ that are semi-regular. Then*

$$\lim_{n\to\infty} P_d(n) = 1$$

Proof. Let $h_d(n)$ be the number of homogeneous elements of $B = \mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2, \ldots, x_n^2)$ of degree greater than or equal to d. Then there are $2^{h_d(n)}$ possible homogeneous sequences (note that we are ignoring order in the sequence). From Lemma 4.3.2 and Proposition 4.3.3 we know that if we pick a spanning set of B_d and add any elements from B_i where $i > d$ then this is a semi-regular sequence. The number of homogeneous elements of B of degree greater than d is

$$h_{d+1}(n) = h_d(n) - (|B_d| - 1).$$

Let S_d be the number of spanning sets of B_d. Then a lower bound on the proportion of semi-regular sequences is given by

$$\frac{S_d 2^{h_{d+1}(n)}}{2^{h_d(n)}} = \frac{S_d}{2^{|B_d|-1}}$$

Let $k = \dim B_d$. Since $1 \leq d < n$ then $k \to \infty$ as $n \to \infty$ and so Proposition 4.3.3, implies that

$$\lim_{k\to\infty} \frac{S_d}{2^{|B_d|-1}} = \lim_{k\to\infty} \frac{S_d}{|\mathcal{P}(B_d \backslash \{0\})|} = 1.$$

□

4.4 Non-Existence of Semi-Regular Sequences over $\mathbb{F}_2$

In this section we prove the following theorem.

Theorem 4.4.1. *Let $d_1, \ldots, d_m$ be a sequence of integers with $d_i \geq 2$ for some $1 \leq i \leq m$.*

Then there exists an N such that for all $n \geq N$, there cannot be a semi-regular sequence $\lambda_1, \ldots, \lambda_m$ of homogeneous polynomials of degrees $d_1, \ldots, d_m$.

In other words, we prove that sequences of a fixed length m and fixed degree $\mathbf{d} = (d_1, \ldots, d_m)$ are never semi-regular for sufficiently large n. This theorem implies that Conjecture 2 in [4] is false.

The idea of the proof is the following. For $\mathbf{d} = (d_1, \ldots, d_m)$, we define the function

$$\tau_{\mathbf{d}}(n) = \operatorname{Ind} \frac{(1+z)^n}{\prod_{i=1}^{m}(1+z^{d_i})}. \tag{4.3}$$

We show that this function is bounded below by a linear function $g(n) = rn + c$, with $r > 1/2$. Suppose that for some j we have that $d_j \geq 2$. Since $r > 1/2$ then there exists N such that for all $n \geq N$

$$\tau_{\mathbf{d}}(n) > \frac{n}{2} + \frac{d_j}{2} + 1.$$

Suppose $\lambda_1, \ldots, \lambda_m$ is a semi-regular sequence of homogeneous polynomials of degrees $d_1, \ldots, d_m$ in $B^{(n)}$, $n \geq N$. Then, by Theorem 3.2.6, $\operatorname{Ind}(\lambda_1, \ldots, \lambda_m) = \tau_{\mathbf{d}}(n) > (n + d_j + 2)/2$. Also, by Theorem 4.2.7 we have that

$$D_{\mathrm{ff}}(\lambda_j) \leq \frac{n + d_j + 2}{2}.$$

Therefore, $D_{\mathrm{ff}}(\lambda_j) < \operatorname{Ind}(\lambda_1, \ldots, \lambda_m)$, but this is not possible for a semi-regular sequence as it was shown in Theorem4.2.8.

Lemma 4.4.2. *Let $f : \mathbb{N} \to \mathbb{R}$ be a non-decreasing function. If there exist n_0, $N \in \mathbb{N}$, and $A \in \mathbb{R}$, such that for all $n \geq n_0$ we have*

$$f(n + N) \geq f(n) + A$$

then there exists a constant c such that

$$f(n) \geq (A/N)n + c$$

for all natural number n.

Proof. Consider the function $g(n) = f(n_0) + (A/N)(n - (n_0 + N))$. Let us show that for all $n \geq n_0$ we have that $f(n) > g(n)$. Let $m \geq n_0$. Write $m - n_0 = lN + b$, where b is an integer $b < N$. By hypothesis we have that

$$f(m) = f(n_0 + b + lN) \geq f(n_0 + b) + lA.$$

Since f is non-decreasing we have that $f(m) \geq f(n_0) + lA$. Now,

$$\begin{aligned} g(m) &= g(n_0 + b + lN) \\ &= f(n_0) + (A/N)(n_0 + b + lN - n_0 - N) \\ &= f(n_0) + A(l - 1) + (A/N)b. \end{aligned}$$

But $b < N$, so $g(m) < f(n_0) + Al \leq f(m)$. Thus, for all $n \geq n_0$ we have that $f(n) > g(n)$. Note that g is defined as

$$g(n) = (A/N)n + k,$$

where $k = f(n_0) - (A/N)(n_0 + N)$. So, for all $n \geq n_0$ we have that $f(n) > (A/N)n + k$. Since we have a finite number of natural numbers less that n_0, then for an appropriate choice of a constant c we have that $f(n) > (A/N)n + c$, for all $n \in \mathbb{N}$. □

Lemma 4.4.3. *For any u between 0 and n, and any $a_j \in \mathbb{R}$*

$$\sum_{j=0}^{n} a_j \binom{n}{j} = \sum_{j=0}^{u-d} \gamma(n, j, d)(a_j + a_{j+d}) + \sum_{j=u-d+1}^{u} \gamma(n, j, d)a_j + \sum_{j=u+1}^{n} \binom{n}{j} a_j$$

Proof. Note that by definition of $\gamma(n, j, d)$, we have that

$$\binom{n}{j} = \gamma(n, j, d) + \gamma(n, j - d, d).$$

Thus

$$\begin{aligned}\sum_{j=0}^{u} a_j \binom{n}{j} &= \sum_{j=0}^{u} (\gamma(n,j,d) + \gamma(n,j-d,d)) a_j \\ &= \sum_{j=0}^{u} \gamma(n,j,d) a_j + \sum_{j=0}^{u} \gamma(n,j-d,d) a_j \\ &= \sum_{j=0}^{u} \gamma(n,j,d) a_j + \sum_{j=0}^{u-d} \gamma(n,j,d) a_{j+d} \\ &= \sum_{j=0}^{u-d} \gamma(n,j,d)(a_j + a_{j+d}) + \sum_{j=u-d+1}^{u} \gamma(n,j,d) a_j\end{aligned}$$

□

Lemma 4.4.4. *Let N, d be natural numbers. Let*

$$\beta(z) = \sum_{j=0}^{\infty} b_j z^j.$$

Suppose that

$$\operatorname{Ind} \beta(z) \geq 1$$

and

$$b_i + b_{i-d} \geq 0$$

for all

$$0 \leq i \leq \operatorname{Ind} \beta(z) + \operatorname{Ind} \frac{(1+z)^N}{1+z^d} - d - 1.$$

Then

$$\operatorname{Ind}(1+z)^N \beta(z) \geq \operatorname{Ind} \beta(z) + \operatorname{Ind} \frac{(1+z)^N}{1+z^d} - d.$$

Proof. Let

$$(1+z)^N \beta(z) = \sum c_i z^i$$

and let $l = \operatorname{Ind} \beta(z)$ and $s = \operatorname{Ind}(1+z)^N/(1+z^d)$. Suppose that $l \geq 1$ and

$$b_i + b_{i-d} \geq 0$$

for all $0 \leq i \leq l+s-d-1$.

We want to show that

$$\mathrm{Ind}(1+z)^N\beta(z) \geq l+s-d.$$

That is, $c_i > 0$ for $0 \leq i \leq l+s-d-1$. Clearly $\mathrm{Ind}(1+z)^N\beta(z) \geq l$. It remains to show that $c_{l+i} > 0$, for $i = 0, \ldots, s-d-1$. For $0 \leq i \leq s-d-1$ we have by above lemma that

$$\begin{aligned} c_{l+i} &= \sum_{j=0}^{N} b_{l+i-j}\binom{N}{j} \\ &= \sum_{j=0}^{s-1-d} \gamma(N,j,d)(b_{l+i-j} + b_{l+i-j-d}) \\ &+ \sum_{j=s-d}^{s-1} \gamma(N,j,d)b_{l+i-j} + \sum_{j=s}^{N}\binom{N}{j}b_{l+i-j}. \end{aligned}$$

For $j = 0, \ldots, s-1$, we have that $\gamma(N,j,d) > 0$, since $s = \mathrm{Ind}(1+z)^N/(1+z^d)$. Also, $b_{l+i-j} + b_{l+i-j-d} \geq 0$, since $l+i-j \leq l+s-d-1$. So

$$\sum_{j=0}^{s-1-d} \gamma(N,j,d)(b_{l+i-j} + b_{l+i-j-d}) \geq 0.$$

Finally, if $j \geq s-d$, then $l+i-j \leq l+(s-d-1)-(s-d) = l-1$, so $b_{l+i-j} > 0$. Hence

$$\sum_{j=s-d}^{s-1} \gamma(N,j,d)b_{l+i-j} + \sum_{j=s}^{N}\binom{N}{j}b_{l+i-j} > 0.$$

Thus, we have shown that $c_i > 0$ for $0 \leq i \leq l+s-d-1$. So

$$\mathrm{Ind}(1+z)^N\beta(z) \geq l+s-d.$$

□

Theorem 4.4.5. *If* $\mathrm{Ind}\,\alpha(z) \geq 1$ *and*

$$\mathrm{Ind}\,\alpha(z) \geq \mathrm{Ind}\,\frac{\alpha(z)}{1+z^d} + \mathrm{Ind}\,\frac{(1+z)^N}{1+z^d} - d$$

then

$$\mathrm{Ind}\,\frac{(1+z)^N\alpha(z)}{1+z^d} \geq \mathrm{Ind}\,\frac{\alpha(z)}{1+z^d} + \mathrm{Ind}\,\frac{(1+z)^N}{1+z^d} - d$$

Proof. Let

$$\alpha(z) = \sum a_i z^i, \quad \frac{\alpha(z)}{1+z^d} = \sum b_i z^i = \beta(z)$$

and let $l = \operatorname{Ind} \beta(z)$ and $s = \operatorname{Ind}(1+z)^N/(1+z^d)$. Suppose that

$$\operatorname{Ind} \alpha(z) \geq \operatorname{Ind} \frac{\alpha(z)}{1+z^d} + \operatorname{Ind} \frac{(1+z)^N}{1+z^d} - d$$

with $\operatorname{Ind} \alpha(z) \geq 1$. In other words, $\operatorname{Ind} \alpha(z) \geq 1$ and

$$\operatorname{Ind} \alpha(z) \geq l + s - d.$$

We want to show that

$$\operatorname{Ind}(1+z)^N \beta(z) \geq l + s - d.$$

Since $\operatorname{Ind} \alpha(z) \geq 1$ then $\operatorname{Ind} \beta(z) \geq 1$. Also, note that

$$b_i + b_{i-d} = a_i > 0$$

for all $0 \leq i \leq l + s - d - 1$, since $\operatorname{Ind} \alpha(z) \geq l + s - d$. Thus, by Lemma 4.4.4 we have that

$$\operatorname{Ind}(1+z)^N \beta(z) \geq l + s - d.$$

□

Lemma 4.4.6. *Let d, N be natural numbers. Then*

$$\operatorname{Ind} \frac{(1+z)^N (1+z)^n}{1+z^d} \geq \operatorname{Ind} \frac{(1+z)^n}{1+z^d} + \operatorname{Ind} \frac{(1+z)^N}{1+z^d} - d$$

for all natural numbers n.

Proof. Consider

$$\frac{(1+z)^n}{1+z^d} = \sum_{i=0}^{\infty} b_i z^i = \beta(z).$$

We want to show that

$$\operatorname{Ind}(1+z)^N \beta(z) \geq \operatorname{Ind} \beta(z) + \operatorname{Ind} \frac{(1+z)^N}{1+z^d} - d.$$

Clearly $\operatorname{Ind}\beta(z) \geq 1$. Also, we have that

$$b_i + b_{i-d} = \binom{n}{i} \geq 0$$

for all i. Thus, the result follows from Lemma 4.4.4. □

Theorem 4.4.7. *Suppose that*

$$r \in \left\{ \frac{1}{n} \left(\operatorname{Ind} \frac{(1+z)^n}{1+z^d} - d \right) \mid n \geq 1 \right\}$$

then there exists a c such that

$$\operatorname{Ind} \frac{(1+z)^n}{1+z^d} \geq rn + c$$

for all n.

Proof. Let

$$r = \frac{1}{N} \left(\operatorname{Ind} \frac{(1+z)^N}{1+z^d} - d \right).$$

Consider the function

$$\tau_{(d)}(k) = \operatorname{Ind} \frac{(1+z)^k}{1+z^d}.$$

By Lemma 4.4.6 we have

$$\begin{aligned} \tau_{(d)}(n+N) &= \operatorname{Ind} \frac{(1+z)^n (1+z)^N}{1+z^d} \\ &\geq \operatorname{Ind} \frac{(1+z)^n}{1+z^d} + \operatorname{Ind} \frac{(1+z)^N}{1+z^d} - d \\ &= \tau_{(d)}(n) + (\tau_{(d)}(N) - d). \end{aligned}$$

By Lemma 4.4.2 there exists c such that

$$\tau_{(d)}(n) \geq \frac{1}{N}(\tau_{(d)}(N) - d)n + c$$

for all n. In other words,

$$\operatorname{Ind} \frac{(1+z)^n}{1+z^d} \geq rn + c$$

for all n. □

Theorem 4.4.8. *Let* $\mathbf{d} = (d_1, \ldots, d_m)$ *and let* $\mathbf{d}' = (d_1, \ldots, d_m, d)$. *Suppose that*

$$r = \frac{1}{N}\left(\operatorname{Ind}\frac{(1+z)^N}{1+z^d} - d\right)$$

for some positive integer N. *Consider the function* $\tau_{\mathbf{d}}(n)$ *as defined in (4.3). If*

$$\tau_{\mathbf{d}}(n) \geq \tau_{\mathbf{d}'}(n) + rN$$

then

$$\tau_{\mathbf{d}'}(n+N) \geq \tau_{\mathbf{d}'}(n) + rN$$

Proof. Consider

$$\alpha(z) = \frac{(1+z)^n}{\prod_{i=1}^m (1+z^{d_i})}.$$

In this case

$$\begin{aligned}
\tau_{\mathbf{d}}(n) &= \operatorname{Ind}\alpha(z) \\
\tau_{\mathbf{d}'}(n) &= \operatorname{Ind}\frac{(1+z)^n}{\prod_{i=1}^m (1+z^{d_i})(1+z^d)} = \operatorname{Ind}\frac{\alpha(z)}{1+z^d} \\
\tau_{\mathbf{d}'}(n+N) &= \operatorname{Ind}\frac{(1+z)^{n+N}}{\prod_{i=1}^m (1+z^{d_i})(1+z^d)} = \operatorname{Ind}\frac{\alpha(z)(1+z)^N}{1+z^d}.
\end{aligned}$$

Also,

$$rN = \operatorname{Ind}\frac{(1+z)^N}{1+z^d} - d.$$

Suppose

$$\tau_{\mathbf{d}}(n) \geq \tau_{\mathbf{d}'}(n) + rN.$$

Thus,

$$\operatorname{Ind}\alpha(z) \geq \operatorname{Ind}\frac{\alpha(z)}{1+z^d} + \operatorname{Ind}\frac{(1+z)^N}{1+z^d} - d.$$

By Theorem 4.4.5

$$\operatorname{Ind}\frac{\alpha(z)(1+z)^N}{1+z^d} \geq \operatorname{Ind}\frac{\alpha(z)}{1+z^d} + \operatorname{Ind}\frac{(1+z)^N}{1+z^d} - d.$$

Therefore,

$$\tau_{\mathbf{d}'}(n+N) \geq \tau_{\mathbf{d}'}(n) + rN.$$

□

Theorem 4.4.9. *Let* $\mathbf{d} = (d_1, \ldots, d_m)$ *and let* $\mathbf{d}' = (d_1, \ldots, d_m, d)$. *Suppose that*

$$s = \frac{1}{N}\left(\operatorname{Ind}\frac{(1+z)^N}{1+z^d} - d\right)$$

for some positive integer N. *Suppose that there exist* $r \geq s$ *and* c *such that*

$$\tau_{\mathbf{d}}(n) \geq rn + c,$$

for all n. *Then there exists* c' *such that*

$$\tau_{\mathbf{d}'}(n) \geq sn + c',$$

for all n.

Proof. Let $\mathbf{d} = (d_1, \ldots, d_m)$ and let $\mathbf{d}' = (d_1, \ldots, d_m, d)$. Suppose that

$$s = \frac{1}{N}\left(\operatorname{Ind}\frac{(1+z)^N}{1+z^d} - d\right)$$

for some positive integer N. Suppose that there exist $r \geq s$ and c such that

$$\tau_{\mathbf{d}}(n) \geq rn + c,$$

for all n. Let us prove that for $c' = \min\{c - 2sN, -sN, 0\}$ we have

$$\tau_{\mathbf{d}'}(n) \geq sn + c',$$

for all n. If $s \leq 0$, the Theorem is true since $c' \geq 0$ and $\tau_{\mathbf{d}'}(n) \geq 0$. Suppose that $s > 0$. Let n be any natural number. We want to show that

$$\tau_{\mathbf{d}'}(n) \geq sn + c'.$$

Let k be the largest positive integer less than or equal to n such that $\tau_{\mathbf{d}'}(k) \geq sk + (c - sN)$, and set $n_1 = k$. If no such positive integer exists, set $n_1 = 0$. If $n_1 = n$, the assertion is true so assume that $n_1 < n$. Write $n - n_1 - 1 = hN + b$ where b is an integer $b < N$. Let $m = n_1 + 1 + jN$ where $0 \leq j \leq h$. Then

$$\tau_{\mathbf{d}'}(m) < sm + (c - sN) \leq rm + (c - sN).$$

Hence $\tau_{\mathbf{d}}(m) \geq \tau_{\mathbf{d}'}(m) + sN$. By Theorem 4.4.8 we have that $\tau_{\mathbf{d}'}(m + N) \geq \tau_{\mathbf{d}'}(m) + sN$. So by iterating this argument,

$$\tau_{\mathbf{d}'}(m) \geq \tau_{\mathbf{d}'}(n_1 + 1) + jsN \geq \tau_{\mathbf{d}'}(n_1) + jsN$$

Hence,

$$\begin{aligned} \tau_{\mathbf{d}'}(n) &\geq \tau_{\mathbf{d}'}(n_1 + 1 + hN) \\ &\geq \tau_{\mathbf{d}'}(n_1) + hsN. \end{aligned}$$

If $n_1 = k$ we have that

$$\begin{aligned} \tau_{\mathbf{d}'}(n) &\geq \tau_{\mathbf{d}'}(n_1) + hsN \\ &\geq s(n_1) + (c - sN) + hsN \\ &= s(n_1 + hN) + (c - sN) \\ &= s(n - 1 - b) + (c - sN) \\ &= sn - s(1 + b) + (c - sN) \\ &\geq sn - sN + (c - sN) \\ &\geq sn + c'. \end{aligned}$$

If $n_1 = 0$ we have

$$\begin{aligned}\tau_{\mathbf{d}'}(n) &\geq \tau_{\mathbf{d}'}(n_1) + hsN \\ &\geq hsN \\ &= s(n-1-b) \\ &= sn - s(1+b) \\ &\geq sn - sN \\ &\geq sn + c'.\end{aligned}$$

□

Theorem 4.4.10. *Let* $\mathbf{d} = (d_1, \ldots, d_m)$. *Suppose that* r *is such that for all* i *there exists an* n_i *such that*

$$r \leq \frac{1}{n_i}\left(\operatorname{Ind}\frac{(1+z)^{n_i}}{1+z^{d_i}} - d_i\right).$$

Then there exists a c *such that*

$$\tau_{\mathbf{d}}(n) = \operatorname{Ind}\frac{(1+z)^n}{\prod_{i=1}^m (1+z^{d_i})} \geq rn + c$$

for all n.

Proof. Let

$$r_i = \frac{1}{n_i}\left(\operatorname{Ind}\frac{(1+z)^{n_i}}{1+z^{d_i}} - d_i\right).$$

Reordering we can suppose that $r_1 \geq r_2 \geq \cdots \geq r_m \geq r$. By Theorem 4.4.7 we have that there exists c_1 such that

$$\tau_{(d_1)}(n) \geq r_1 n + c_1,$$

for all n. By Theorem 4.4.9 we have that there exists c_2 such that

$$\tau_{(d_1,d_2)}(n) \geq r_2 n + c_2,$$

for all n. By iterating this argument we have that there exists c such that

$$\tau_{\mathbf{d}}(n) \geq rn + c,$$

for all n. □

Lemma 4.4.11. *Let d be a natural number. Then there exists M such that for all $n \geq M$*

$$\binom{2n}{n+d-j} - \binom{2n}{n-j} + \binom{2n}{n-j-d} - \binom{2n}{n-j-2d} > 0$$

for all $0 \leq j \leq d - \lfloor d/2 \rfloor - 1$.

Proof. Let $p = \lfloor d/2 \rfloor$. Note that for $0 \leq j \leq d - p - 1$

$$\begin{aligned}
&\binom{2n}{n+d-j} - \binom{2n}{n-j} + \binom{2n}{n-j-d} - \binom{2n}{n-j-2d} \\
&\geq \binom{2n}{n+d} - \binom{2n}{n} + \binom{2n}{n-2d+p+1} - \binom{2n}{n-2d}.
\end{aligned}$$

Now,

$$\begin{aligned}
&\binom{2n}{n+d} - \binom{2n}{n} + \binom{2n}{n-2d+p+1} - \binom{2n}{n-2d} \\
&= \frac{(2n)!}{(n+d)!(n-d)!} - \frac{(2n)!}{n!n!} + \frac{(2n)!}{(n-2d+p+1)!(n+2d-p-1)!} \\
&- \frac{(2n)!}{(n-2d)!(n+2d)!}.
\end{aligned}$$

Note that

$$\begin{aligned}
&\frac{1}{(n+d)!(n-d)!} - \frac{1}{n!n!} + \frac{1}{(n-2d+p+1)!(n+2d-p-1)!} \\
&- \frac{1}{(n-2d)!(n+2d)!} \\
&= \frac{q(n)}{(n+2d-p-1)!(n+2d)!},
\end{aligned}$$

where

$$\begin{aligned}
q(n) = &\prod_{i=1}^{d}(n+d+i) \prod_{i=1}^{3d-p-1}(n-d+i) - \prod_{i=1}^{2d}(n+i) \prod_{i=1}^{2d-p-1}(n+i) \\
&+ \prod_{i=1}^{4d-p-1}(n-2d+p+1+i) - \prod_{i=1}^{4d-p-1}(n-2d+i).
\end{aligned}$$

Clearly $q(n)$ is a polynomial in n of degree at most $4d-p-1$. The coefficient of n^{4d-p-1} is easily seen to be zero and that of n^{4d-p-2} is

$$\begin{aligned}
&\left(d^2+\frac{d(d+1)}{2}+(3d-p-1)(-d)+\frac{(3d-p-1)(3d-p)}{2}\right)\\
&-\left(\frac{(2d)(2d+1)}{2}+\frac{(2d-p-1)(2d-p)}{2}\right)\\
&+\left((4d-p-1)(-2d+p+1)+\frac{(4d-p-1)(4d-p)}{2}\right)\\
&-\left((4d-p-1)(-2d)+\frac{(4d-p-1)(4d-p)}{2}\right)\\
&=4dp-d^2-p^2+4d-2p-1,
\end{aligned}$$

which is positive for all $d \geq 1$. Thus the leading coefficient of $q(n)$ is positive and $q(n)$ is positive for all $n \geq M$, for some M. □

Lemma 4.4.12. *Let n, d be natural numbers. Then*

$$\gamma(2n,k,d) > 0$$

for all $0 \leq k \leq n + \lfloor d/2 \rfloor$.

Proof. By definition we have

$$\gamma(2n,k,d) = \sum_{j=0}^{\lfloor k/d \rfloor} (-1)^j \binom{2n}{k-jd}.$$

We know that $\binom{2n}{j}$ is strictly increasing when $0 \leq j \leq n$, therefore

$$\gamma(2n,k,d) > 0$$

for all $0 \leq k \leq n$. Now, for $n \leq k \leq n + \lfloor d/2 \rfloor$ we have

$$\gamma(2n,k,d) = \binom{2n}{k} - \binom{2n}{k-d} + \gamma(2n,k-2d,d).$$

If $k \leq n + \lfloor d/2 \rfloor$, then $k - 2d \leq n$. Thus

$$\gamma(2n,k-2d,d) > 0$$

for all $n \leq k \leq n + \lfloor d/2 \rfloor$. In order to finish let us show that

$$\binom{2n}{k} - \binom{2n}{k-d} \geq 0$$

for all $n \leq k \leq n + \lfloor d/2 \rfloor$. If $n \leq k \leq n + \lfloor d/2 \rfloor$ then

$$n - d \leq k - d \leq n + \lfloor d/2 \rfloor - d \leq n - \lfloor d/2 \rfloor$$

and

$$n - \lfloor d/2 \rfloor \leq 2n - k \leq n.$$

So, for $n \leq k \leq n + \lfloor d/2 \rfloor$ we have that

$$\binom{2n}{n-d} \leq \binom{2n}{k-d} \leq \binom{2n}{n - \lfloor d/2 \rfloor}$$

and

$$\binom{2n}{n - \lfloor d/2 \rfloor} \leq \binom{2n}{2n-k} \leq \binom{2n}{n}.$$

Thus, for $n \leq k \leq n + \lfloor d/2 \rfloor$

$$\begin{aligned}
\binom{2n}{k} - \binom{2n}{k-d} &= \binom{2n}{2n-k} - \binom{2n}{k-d} \\
&\geq \binom{2n}{n - \lfloor d/2 \rfloor} - \binom{2n}{n - \lfloor d/2 \rfloor} \\
&= 0.
\end{aligned}$$

The result is proved. □

Theorem 4.4.13. *Let d be a natural number. There exists K such that for all $n \geq K$ we have*

$$\operatorname{Ind} \frac{(1+z)^n}{1+z^d} > \frac{n}{2} + d$$

Proof. First let us prove that there exists M such that for all $n \geq M$ we have

$$\operatorname{Ind} \frac{(1+z)^{2n}}{1+z^d} > \frac{2n}{2} + d$$

By equation (4.1), we need to show that there exists M such that for all $n \geq M$ we have

$$\gamma(2n, k, d) > 0,$$

for all $0 \leq k \leq n + d$. By Lemma 4.4.12 we have that for any n

$$\gamma(2n, k, d) > 0, \text{ for all } 0 \leq k \leq n + \lfloor d/2 \rfloor. \tag{4.4}$$

It remains to show that there exists M such that for all $n \geq M$

$$\gamma(2n, n + d - j, d) > 0$$

for all $0 \leq j \leq d - \lfloor d/2 \rfloor - 1$. For all $0 \leq j \leq d - \lfloor d/2 \rfloor - 1$, we have that

$$\begin{aligned}\gamma(2n, n + d - j, d) = &\binom{2n}{n + d - j} - \binom{2n}{n - j} \\ &+ \binom{2n}{n - j - d} - \binom{2n}{n - j - 2d} \\ &+ \gamma(2n, n - j - 3d, d).\end{aligned}$$

By Lemma 4.4.11, we have that there exist M such that for all $n \geq M$

$$\binom{2n}{n + d - j} - \binom{2n}{n - j} + \binom{2n}{n - j - d} - \binom{2n}{n - j - 2d} > 0$$

for all $0 \leq j \leq d - \lfloor d/2 \rfloor - 1$. Also, by (4.4) we have that

$$\gamma(2n, n - j - 3d, d) > 0, \text{ for all } 0 \leq j \leq d - \lfloor d/2 \rfloor - 1.$$

Therefore, for all $n \geq M$

$$\gamma(2n, k, d) > 0, \text{ for all } n + \lfloor d/2 \rfloor + 1 \leq k \leq n + d. \tag{4.5}$$

Thus from (4.4) and (4.5) we have that for all $n \geq M$

$$\gamma(2n, k, d) > 0,$$

for all $0 \leq k \leq n + d$. In other words, for all $n \geq M$

$$\operatorname{Ind} \frac{(1+z)^{2n}}{1+z^d} \geq \frac{2n}{2} + d + 1 > \frac{2n}{2} + d. \tag{4.6}$$

So, for all $n \geq M$

$$\operatorname{Ind} \frac{(1+z)^{2n+1}}{1+z^d} \geq \operatorname{Ind} \frac{(1+z)^{2n}}{1+z^d} \geq \frac{2n}{2} + d + 1 > \frac{2n+1}{2} + d. \tag{4.7}$$

From (4.6) and (4.7) we have that

$$\operatorname{Ind} \frac{(1+z)^{n}}{1+z^d} > \frac{n}{2} + d$$

for all $n \geq K$, where $K = 2M + 1$. □

Now, let us prove the main theorem of this section.

Theorem 4.4.14. *Let* $\mathbf{d} = (d_1, \ldots, d_m)$*, with* $d_j \geq 2$ *for some* $1 \leq j \leq m$*. Then there exists an* N *such that for all* $n \geq N$*, there are no semi-regular sequences of type* $\mathbf{d}$ *in* $B^{(n)}$*.*

Proof. By Theorem 4.4.13, for all $0 \leq i \leq m$ there exists an n_i such that

$$\operatorname{Ind} \frac{(1+z)^{n_i}}{1+z^{d_i}} > \frac{n_i}{2} + d_i.$$

Set

$$r_i = \frac{1}{n_i}\left(\operatorname{Ind} \frac{(1+z)^{n_i}}{1+z^{d_i}} - d_i\right) > \frac{1}{2}$$

and let $r = \min r_i$. By Theorem 4.4.10 there exists c such that

$$\tau_{\mathbf{d}}(n) \geq rn + c, \text{ for all } n.$$

Suppose that for some j we have that $d_j \geq 2$. Since $r > 1/2$, there exists N such that for all $n \geq N$

$$\tau_{\mathbf{d}}(n) > \frac{n}{2} + \frac{d_j}{2} + 1.$$

Suppose $\lambda_1, \ldots, \lambda_m$ is a semi-regular sequence of homogeneous polynomials of degrees $d_1, \ldots, d_m$ in $B^{(n)}$, $n \geq N$. Thus, by Theorem 3.2.6, $\mathrm{Ind}(\lambda_1, \ldots, \lambda_m) = \tau_{\mathbf{d}}(n) > (n + d_j + 2)/2$. Since $d_j \geq 2$, Theorem 4.2.7 tells us that

$$D_{\mathrm{ff}}(\lambda_j) \leq \frac{n + d_j + 2}{2}.$$

This would imply that $D_{\mathrm{ff}}(\lambda_j) < \mathrm{Ind}(\lambda_1, \ldots, \lambda_m)$, but by Theorem 4.2.8 this is not possible for a semi-regular sequence. $\square$

CHAPTER 5

Conclusions and Future Work

Since the introduction of the concept of a semi-regular sequence over $\mathbb{F}_2$, it has been conjectured that such sequences are in some sense "generic". However little concrete progress has been made towards proving this conjecture. In fact even in one of the simplest and most important cases, that of quadratic sequences of length n in n variables, the question of the *existence* of semi-regular sequences for all n remains open. In this work I present more reliable proofs for the Hilbert characterization of semi-regularity and give a new homological characterization of semi-regularity over $\mathbb{F}_2$. Also, I proved some results on the existence and non-existence of semi-regular sequences over $\mathbb{F}_2$. I looked at the most elementary case, that of semi-regular elements (or sequences of length one). It was observed by T. J. Hodges and J. Schlather homogeneous element of degree d can only be semi-regular if $n \leq 3d$. I established precisely when the symmetric element

$$\sigma_{d,n} = \sum_{1 \leq i_1 < \cdots < i_d \leq n} x_{i_1} \cdots x_{i_d}$$

is semi-regular. In particular when $d = 2^t$, $\sigma_{d,n}$ is semi-regular for all $d \leq n \leq 3d$ establishing that the bound $n \leq 3d$ is sharp for infinitely many n. For the general case of existence of semi-regular sequences the authors of [4] conjecture that the proportion $\pi(n, m, d_1, \ldots, d_m)$ of semi-regular sequences over $\mathbb{F}_2$ in the set $E(n, m, d_1, \ldots, d_m)$ of algebraic systems of m equations of degrees $d_1, \ldots, d_m$ in n variables tends to 1 as n tends to ∞.

I show that this conjecture is false. In fact, the opposite is true. I show that for a fixed choice of $(m, d_1, \ldots, d_m)$, we have that

$$\lim_{n\to\infty} \pi(n, m, d_1, \ldots, d_m) = 0$$

This results presented in this work represent the first significant progress about the existence of semi-regular sequences over $\mathbb{F}_2$ since this concept was introduced in [3, 5, 4, 6].

On the other side, little progress has been made proving the observed fact that "most" sequences are semi-regular. What we would like to show is something like the following. There exists an ϵ such that if $m(n) = \lfloor \alpha n \rfloor + c$, then the proportion of semi-regular sequences of length $m(n)$ in n variables tends to one as n tends to infinity whenever $\alpha > \epsilon$. This appears to be a hard problem. Looking at Table 4.1 there do appear to be sporadic values of (n, m) for which the proportion of semi-regular elements is low (such as $(n, m) = (10, 12), (11, 15)$ and $(15, 14)$). These low proportions correspond precisely to values of (n, m) for which the coefficient of $(1 + z)^n/(1 + z^2)^m$ is zero at the index. If this phenomenon can occur for arbitrarily large values of n and m, then it is possible that Conjecture 4 will be false.

Future Research

First, it remains a problem to even define semi-regular sequences on fields of characteristic $q > 2$. A possible way to do this is modify the definition given in [3, 5, 4, 6] and try to generalize the homological characterization for semi-regular sequences over the field $\mathbb{F}_2$ that we give in Section 3.2.2. I would also like to solve the problem about the existence of semi-regular quadratic sequences of length n in n variables, a problem that remains open and that is of important interest in multivariate cryptosystems.

On the other hand, the degree of regularity of a semi-regular system is well known [6]. However, the degree of regularity of a system that is not semi-regular is hard to determine

precisely. In Section 4.2.5 it is conjectured that for an arbitrary sequence $\lambda_1, \ldots, \lambda_m$ the degree of regularity is bounded below by $\operatorname{Ind} T_{n,m}(z)$. All known evidence points to this result being true. I am interested to work in this problem because it is important to know the degree of regularity of a system of polynomials since this is related to the complexity of the Gröbner basis approach to solving these systems and it has been observed than many sequences that arise in cryptography, such as those arising from the Hidden Field Equation cryptosystems, are not semi-regular.

Bibliography

[1] M. Atiyah and I. Macdonald. *Introduction to commutative algebra*, volume 2. Addison-Wesley Reading, 1969.

[2] Nadia Ben Atti, Gema M Diaz-Toca, and Henri Lombardi. The berlekamp-massey algorithm revisited. *Applicable Algebra in Engineering, Communication and Computing*, 17(1):75–82, 2006.

[3] M. Bardet. *Étude des systèmes algébriques surdéterminés. Applications aux codes correctuers et la cryptograhie.* PhD thesis, Université Paris V!, 2004.

[4] M. Bardet, J. C. Faugère, and B. Salvy. Complexity of Gröbner basis computation for semi-regular overdetermined sequences over $\mathbb{F}_2$ with solutions in $\mathbb{F}_2$. *INRIA Research Report 5049*, 2003.

[5] M. Bardet, J. C. Faugère, and B. Salvy. On the complexity of gröbner basis computation of semi-regular overdetermined algebraic equations. *Proc. ICPSS International Conference on Polynomial System Solving Paris*, pages 71–75, 2004.

[6] M. Bardet, J. C. Faugère, B. Salvy, and B. Y. Yang. Asymptotic expansion of the degree of regularity for semi-regular systems of equations. *MEGA 2005 Sardinia (Italy).*

[7] B. Buchberger. *Ein Algorithmus zum Affinder der Basiselemente der Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, University of Innsbruck, 1965.

[8] B. Buchberger. Gröbner-bases: An algorithmic method in polynomial ideal theory. *N. Bose, editor, Multidimensional Systems Theory*, pages 184–232, 1985.

[9] J. Buchmann, J. Ding, M. S. E. Mohamed, W. S. A. M. Mohamed, and R.-P. Weinmann. Mutant xl. *First International Conference on Symbolic Computation and Cryptography SCC*, 2008.

[10] C Chester, B Friedman, and F Ursell. An extension of the method of steepest descents. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 53, pages 599–611. Cambridge Univ Press, 1957.

[11] N. Courtois, A. Klimov, J. Patarin, and A. Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. *Eurocrypt 2000, LNCS*, 1807:392–407, 2000.

[12] Cox David, Little John, and O'Shea Donal. Ideals varieties and algorithms: an introduction to computational algebraic geometry and commutative algebra, 1996.

[13] Nicolaas Govert De Bruijn. *Asymptotic methods in analysis*, volume 4. Courier Corporation, 1970.

[14] C. Diem. Bounded regularuty. *J. of Algebra*, 423:1143–1160, 2015.

[15] H. Ding, T. Hodges, and K. Kruglov. Growth of the ideal generated by a quadratic boolean function. In *PQCrypto'10*, pages 13–27, 2010.

[16] J. Ding, T. J. Hodges, V. Kruglov, D. Schmidt, and S. Tohaneanu. Growth of the ideal generated by a multivariate quadratic function over gf(3). *J. of Algebra and Its Applications*, 12, 2013.

[17] J. Ding and D. Schmidt. Rainbow, a new multivariable polynomial signature scheme. *ACNS 2005. LNCS*, 3531:164–175, 2005.

[18] D. Eisenbud. *Commutative Algebra: with a view toward algebraic geometry*, volume 150. Springer Science & Business Media, 1995.

[19] J. C. Faugère. A new efficient algorithm for computing Gröbnerbases without reduction to zero (f5). *ISSAC 202*, pages 75–83.

[20] J. C. Faugère. A new efficient algorithm for computing Gröbnerbases (f4). *Pure App. Alg.*, 139:61–88, 1999.

[21] J. C. Faugère and A. Joux. Algebraic cryptanalysis of hidden field equation (hfe) cryptosystems using gr´obner bases. *Advances in Cryptology CRYPTO 2003, LNC*, 2729:4460, 2003.

[22] M. Garey and D. Johnson. Computers and intractability, a guide to the theory of np-completeness. *W. H. Freeman New York*, 1979.

[23] J. L. Gross. Combinatorial methods with computer applications. *Chapman and Hall/CRC*, 2007.

[24] T. J. Hodges, S. Molina, and J. Schlather. On the existance of semi-regular sequences. *submitted*, Available under http://arxiv.org/abs/1412.7865.

[25] T. J. Hodges, C. Petit, and J. Schlather. First fall degree and weil descent. *Finite Fields and Their Applications*, 30:155–177, 2014.

[26] V. Kruglov. *Growth of the ideal generated by a quadratic multivariate function.* PhD thesis, University of Cincinnati, USA, 2010.

[27] S. Lang. Algebra revised third edition. *GRADUATE TEXTS IN MATHEMATICS-NEW YORK-*, 2002.

[28] Daniel Lazard. Gröbner bases, gaussian elimination and resolution of systems of algebraic equations. In *Computer algebra*, pages 146–156. Springer, 1983.

[29] R. Lidl and H. Niederreiter. Finite fields, encyclopedia of mathematics and its applications 20. *Cambridge University Press*, 1997.

[30] T. Matsumoto and H. Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. *Advances in Cryptology - Eurocrypt88. LNCS*, 330:419–453, 1988.

[31] K. Pardue. Generic sequences of polynomials. *J. of Algebra*, 324:579–590, 2010.

[32] J. Patarin. Hidden field equations (hfe) and isomorphisms of polynomials (ip): two new families of asymmetric algorithms. *Advances in Cryptology - Eurocrypt96. LNCS*, 1070:33–48, 1996.

[33] J. Patarin, N. Courtois, and L. Goubin. Flash, a fast multivariate signature algorithm. *CT-RSA 2001. LNCS*, 2020:297307, 2001.

[34] B. Yang and J. Chen. All in the xl family: Theory and practice. In *ICISC 2004. LNCS*, pages 67–86. Springer, 2005.

[35] B. Yang, J Chen, and N. Courtois. On asymptotic security estimates in xl and gröbner bases-related algebraic cryptanalysis. In *ICICS 2004, LNCS 3269:410413*, pages 401–413. Springer-Verlag, 2004.

[36] Bo-Yin Yang and Jiun-Ming Chen. Theoretical analysis of xl over small fields. In *Information Security and Privacy*, pages 277–288. Springer, 2004.